Algorithmic Number Theory

S. Arun-Kumar

December 1, 2002

Contents

Part I

Lectures

Chapter 1

Lecture-wise break up

L. No.	Date	Topic	Scribe
1	01 Aug 02	Divisibility and Euclidean Algorithm	S. Arun-Kumar
2	05 Aug 02	Fibonacci Numbers	S. Arun-Kumar
3	08 Aug 02	Finite Continued Fractions	S. Arun-Kumar
4	12 Aug 02	Simple Infinite Continued Fractions	Anuj Saxena
5	14 Aug 02	Approximations of Irrationals (Hurwitz's theorem)	Keshav Kunal
6	19 Aug 02	Quadratic Irrationals (Periodic Continued Fractions)	Akrosh Gandhi
7	22 Aug 02	Primes and the Infinitude of primes	Ashish Rastogi
8	26 Aug 02	Tchebychev's theorem ($\frac{\pi(x)}{\frac{x}{lnx}}$ is bounded)	Tariq Aftab
9	02 Sep 02	Linear Congruences, Fermat's little theorem and CRT	Rahul Gupta
10	05 Sep 02	Euler's ϕ function, Generalization of FLT and CRT	Bipin Kumar Tripathi
11	09 Sep 02	Using CRT to compute with large numbers	Chandana Deepti
12	12 Sep 02	Congruences of Higher Degree	Satish Parvataneni
13	16 Sep 02	Equations with Prime Moduli	Hitesh Chaudhary
14	19 Sep 02	Primitive Roots and Euler's Criterion	Sai Pramod Kumar
15	23 Sep 02	Quadratic Reciprocity	Dhan M Nakka
16	26 Sep 02	Primes are in P	Akshat Verma
17	30 Sep 02	Applications of Quadratic Reciprocity	Vipul Jain
18	03 Oct 02	The Jacobi Symbol	Gaurav Gupta
19	17 Oct 02	Elementary Algebraic Concepts	Mayank Kumar
20	21 Oct 02	Sylow's Theorem	Amit Agarwal
21	24 Oct 02	Finite Abelian Groups and Dirichlet characters	Tushar Chaudhary
22	28 Oct 02	Dirichlet Products	

Chapter 2

Divisibility and the Euclidean Algorithm

Definition 2.1 *For integers a and b, $b \neq 0$, b is called a* **divisor** *of a, if there exists an integer c such that $a = bc$. A number other than 1 is said to be a* **prime** *if its only divisors are 1 and itself. An integer other than 1 is called* **composite** *if it is not prime.*

Notation.

1. $b|a$ means b is a divisor of a.
2. $b \not| a$ means b is not a divisor of a.

Fact 2.1 *The following are easy to show.*

1. $1|a$ *for all* $a \in \mathbb{Z}$,
2. $a|a$ *for all* $a \neq 0$,
3. $a|b$ *implies* $a|bc$, *for all* $c \in \mathbb{Z}$,
4. $a|b$ *and* $b|c$ *implies* $a|c$,
5. $a|b$ *and* $a|c$ *implies* $a|b \pm c$,
6. *Every prime is a positive integer. 2 is the smallest prime.*

Theorem 2.2 *The set of primes is infinite.*

Proof outline: Assume the set of primes is finite and let them be $p_1, \ldots, p_k$, for some $k \geq 1$. Now consider the number $n = \prod_{i=1}^{k} p_i + 1$. It is easy to see that none of the primes $p_1, \ldots, p_k$ is a divisor of n and n is larger than any of them. Hence n must be a prime, contradicting the assummption. □

Theorem 2.3 The Fundamental theorem of arithmetic. *Every integer $n > 1$ may be expressed uniquely in the form $\prod_{i=1}^{k} p_i^{\alpha_i}$, for some $k \geq 0$, where p_i, $1 \leq i \leq k$ are the primes in order and $\alpha_i \geq 0$ for $1 \leq i \leq k$.*

Theorem 2.4 The division algorithm *Given any two integers a, $b > 0$, there exist unique integers q, r with $0 \leq r < b$, such that $a = bq + r = b(q+1) - (b-r)$ and $min(r, b-r) \leq \frac{b}{2}$. q is the* **quotient** *and r the* **remainder** *obtained by dividing b into a.*

Notation. We use the notation $adivb$ and $amodb$ to denote the quotient q and remainder r (respectively) obtained by dividing b into a.

Definition 2.2 *$d \in \mathbb{Z}$ is a* **common divisor** *of $a, b \in \mathbb{Z}$ if $d|a$ and $d|b$. d is called the* **greatest common divisor (GCD)** *of a and b if it is the largest among the common divisors of a and b.*

Notation.

1. $p^\alpha || a$ means $p^\alpha | a$ and $p^{\alpha+1} \not| \, a$.
2. $gcd(a, b)$ denotes the GCD of a and b.

Theorem 2.5 *There exist integers x, y such that $gcd(a, b) = ax + by$, provided $a > 0$ or $b > 0$.*

Proof outline: The proof depends upon the following claims which are easily proven.

1. $S = \{au + bv | au + bv > 0, u, v \in \mathbb{Z}\} \neq \emptyset$.
2. $d = \min S$ is a common divisor of a and b.
3. $d = gcd(a, b)$.

□

Corollary 2.6 *$T = \{ax + by | x, y \in \mathbb{Z}\}$ is exactly the set of all multiples of $d = gcd(a, b)$.*

Theorem 2.7 The Euclidean theorem *If $a = bq + r$ then $gcd(a, b) = gcd(b, r)$.*

Proof outline: Let $d = gcd(a, b)$. the the following are easy to prove.

1. d is a common divisor of b and r.
2. Let $c = gcd(b, r)$. Then $c|a$ and $c \leq d$.

□

Note: It is not necessary for q and r chosen in the above theorem to be the quotient and remainder obtained by dividing b into a. The theorem holds for any integers q and r satisfying the equality $a = bq + r$.

The Euclidean theorem directly gives us an efficient algorithm to compute the GCD of two numbers.

Algorithm 2.1 The Euclidean Algorithm

```
algorithm euclid(a, b)
begin
    if (b=0) then a
    else euclid (b, a mod b)
end
```

Chapter 3

Fibonacci Numbers

Theorem 3.1 *$gcd(F_{n+1}, F_n) = 1$ for all $n \geq 1$.*

Proof: For $n = 1$, the claim is clearly true. Assume for some $n > 1$, $gcd(F_{n+1}, F_n) \neq 1$ Let $k \geq 2$ be the smallest integer such that $gcd(F_{k+1}, F_k) = d \neq 1$. Clearly since $F_{k+1} = F_k + F_{k-1}$, it follows that $d|F_{k-1}$, which contradicts the assumption. □

Theorem 3.2 *$F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$, for all $m > 0$ and $n \geq 0$.*

Proof outline: By induction on n for each fixed m. □

Theorem 3.3 *For $m \geq 1, n \geq 1$, $F_m|F_{mn}$.*

Proof outline: By induction on n. □

Lemma 3.1 *If $m = nq + r$, for $m, n > 0$, then $gcd(F_m, F_n) = gcd(F_n, F_r)$.*

Proof: We have $F_m = F_{nq+r} = F_{nq-1}F_r + F_{nq}F_{r+1}$ by theorem 3.2. Hence $gcd(F_m, F_n) = gcd(F_{nq-1}F_r + F_{nq}F_{r+1}, F_n)$. We know that $gcd(a + c, b) = gcd(a, b)$ when $b|c$. Hence since $F_n|F_{nq}$, we have $F_n|F_{nq}F_{r+1}$.

Claim. $gcd(F_{nq-1}, F_n) = 1$. If $d = gcd(F_{nq-1}, F_n)$, then $d|F_{nq-1}$ and $d|F_n$ which implies $d|F_{nq}$. But $d|F_{nq-1}$ and $d|F_{nq}$ implies $d = 1$.

Hence

$$\begin{aligned} & gcd(F_m, F_n) \\ = \; & gcd(F_{nq-1}F_r + F_{nq}F_{r+1}, F_n) \\ = \; & gcd(F_{nq-1}F_r, F_n) \\ = \; & gcd(F_r, F_n & & \text{since } gcd(F_{nq-1}, F_n) = 1 \\ = \; & gcd(F_n, F_r \end{aligned}$$

□

Theorem 3.4 *The GCD of two fibonacci numbers is again a fibonacci number. In fact, $gcd(F_n, F_m) = F_{gcd(n,m)}$.*

Proof: Lemma 3.1 essentially tells us that something very similar to the Euclidean algorithm works here too. The correpondence is made clear by the following.

$$\begin{array}{lclccl} & & & & & gcd(F_n, F_m) \\ n & = & mq_0 + r_2 & \text{implies} & = & gcd(F_m, F_{r_2}) \\ m & = & r_2 q_1 + r_3 & \text{implies} & = & gcd(F_{r_2}, F_{r_3}) \\ & \vdots & & & \vdots & \\ r_{n-2} & = & r_{n-1}q_{n-2} + r_n & \text{implies} & = & gcd(F_{r_{n-1}}, F_{r_n}) \\ r_{n-1} & = & r_n q_{n-1} + 0 & & = & F_{r_n} \end{array}$$

Since $r_n | r_{n-1}$ we have $F_{r_n} | F_{r_{n-1}}$. Hence $gcd(F_n, F_m) = F_{r_n} = F_{gcd(n,m)}$. □

Corollary 3.5 Converse of theorem 3.3. *$F_m | F_n$ implies $m|n$.*

Proof: $F_m | F_n$ implies $F_m = gcd(F_m, F_n) = F_{gcd(m,n)}$ which in turn implies $m = gcd(m, n)$ whence $m|n$. □

Theorem 3.6 *The following identities hold.*

1.
$$\sum_{i=1}^{n} F_i = F_{n+2} - 1$$

2.
$$F_n^2 = F_{n+1}F_{n-1} + (-1)^{n-1}$$

3.
$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$$

where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$ are the solutions of the quadratic $x^2 = x + 1$.

Proof:

1.
$$\begin{array}{lcl} F_1 & = & F_3 - F_2 \\ F_2 & = & F_4 - F_3 \\ & \vdots & \\ F_n & = & F_{n+2} - F_{n+1} \end{array}$$

Adding the above equations and cancelling all F_i, $3 \le i \le n+1$, $\sum_{i=1}^{n} F_i = F_{n+2} - F_2 = F_{n+2} - 1$.

2. Consider
$$\begin{array}{cll} & F_n^2 - F_{n+1}F_{n+2} & \ldots(1) \\ = & F_n(F_{n-1} + F_{n-2}) - F_{n+1}F_{n-1} & \\ = & (F_n - F_{n+1})F_{n-1} + F_nF_{n-2} & \\ = & -F_{n-1}F_{n-1} + F_nF_{n-2} & \\ = & (-1)(F_{n-1}^2 - F_nF_{n-2}) & \ldots(2) \end{array}$$

(1) and (2) are essentially the same except for the initial sign and the fact that subscripts have all been reduced by 1. We may continue this process of reducing the subscripts with alternating signs to obtain $F_n^2 - F_{n+1}F_{n-1} = (-1)^{n-1}(F_1 - F_2F_0) = (-1)^{n-1}$.

3. By induction on n. For $n = 1$ it is trivial. Assuming $F_n = \dfrac{\alpha^n - \beta^n}{\sqrt{5}}$, we have

$$\begin{aligned} & F_{n+1} \\ = \; & F_n + F_{n-1} \\ = \; & \frac{\alpha^n - \beta^n}{\sqrt{5}} + \frac{\alpha^{n-1} - \beta^{n-1}}{\sqrt{5}} \\ = \; & \frac{\alpha^{n-1}(\alpha + 1) - \beta^{n-1}(\beta + 1)}{\sqrt{5}} \\ = \; & \frac{\alpha^{n+1} - \beta^{n+1}}{\sqrt{5}} \end{aligned}$$

The last step is obtained from the previous step using the identities $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$, since they are both solutions of the equation $x^2 = x + 1$.

□

Theorem 3.7 *Every positive integer may be expressed as the sun of distinct fibonacci numbers.*

Proof: We actually prove the following claim.

Claim. Every number in the set $\{1, 2, \ldots, F_n - 1\}$ is a sum of distinct numbers from $\{F_1, F_2, \ldots, F_{n-2}\}$.

We prove this claim by induction on n. For $n = 1$ it is trivial. Assume the claim is true for $n = k$. Choose any N such that $F_k < N < F_{k+1}$. We have $N - F_{k-1} < F_{k+1} - F_{k-1} = F_k$. By the induction hypothesis, $N - F_{k-1}$ is representable as a sum of distinct numbers from $\{F_1, F_2, \ldots, F_{k-2}\}$. By adding F_k we get that N is representable as a sum of distinct numbers from $\{F_1, F_2, \ldots, F_{k-2}, F_{k-1}\}$ □

Chapter 4

Continued Fractions

Definition 4.1 *A* **continued fraction** *is of the form*

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{\ddots}}}$$

where $a_0 \in \mathbb{R}$ *and* $a_1, a_2, \ldots, b_1, b_2, \ldots$ *are all positive reals.*

Example 4.1 *The following simple infinite continued fraction represents the real number* $\sqrt{13}$. *(Prove it!)*

$$3 + \cfrac{4}{6 + \cfrac{4}{6 + \cfrac{4}{\ddots}}}$$

Definition 4.2 *Our interest will be restricted to continued fractions where* $b_1 = b_2 = b_3 = \ldots = 1$. *Such a continued fraction is denoted by the list* $[a_0; a_1, a_2, \ldots]$. *It is said to be* **finite** *if this list is finite, otherwise it is called* **infinite**. *It is said to be* **simple** *if all the elements of the list are integers. We often use the abbreviation* **SFCF** *to refer to "simple finite continued fractions".*

Fact 4.1 *Any SFCF represents a rational number.*

Theorem 4.2 *Every rational number may be expressed as a simple finite continued fraction.*

Corollary 4.3 *If* $0 < a/b < 1$ *then* $a_0 = 0$.

Fact 4.4 *If* $a/b = [a_0; a_1, a_2, \ldots, a_n]$, *then if* $a_n > 1$, *we may also write* $a/b = [a_0; a_1, a_2, \ldots, a_n - 1, 1]$. *Hence every rational number has at most* two *representations as a SFCF*

Example 4.2 $F_{n+1}/F_n = [1; 1, 1, \ldots, 1, 2] = [1; 1, 1, \ldots, 1, 1, 1]$ *where* F_{n+1} *and* F_n *are consecutive fibonacci numbers.*

Definition 4.3 *Let $a/b = [a_0; a_1, a_2, \ldots, a_n]$ be a SFCF. Then $C_k = [a_0; a_1, a_2, \ldots, a_k]$ for $0 \leq k \leq n$ is called the* k**-th convergent** *of a/b.*

Note.

1. We will often regard SFCFs as being interchangeable with their values as rational nmumbers.
2. It is clear from fact 4.1 and theorem 4.2 that convergents too may be regarded both as SFCFs and as rational numbers.

Fact 4.5 *C_k with a_k replaced by $a_k + \dfrac{1}{a_{k+1}}$ yields C_{k+1}.*

Definition 4.4 *For $[a_0; a_1, a_2, \ldots, a_n]$ let*

$$\begin{array}{lll} p_0 & = & a_0 \\ p_1 & = & a_1 a_0 + 1 \\ p_k & = & a_k p_{k-1} + p_{k-2} \end{array} \qquad \begin{array}{lll} q_0 & = & 1 \\ q_1 & = & a_1 \\ q_k & = & a_k q_{k-1} + q_{k-2} \quad \textit{for } 2 \leq k \leq n \end{array}$$

Lemma 4.1 *For the SFCF $[a_0; a_1, a_2, \ldots, a_n]$, $C_k = \dfrac{p_k}{q_k}$ for $0 \leq k \leq n$.*

Proof outline: By induction on k □

Note. In the sequel we will assume unless otherwise stated, that we have a SFCF $[a_0; a_1, a_2, \ldots, a_n]$ whose convergents are C_k and in each case $C_k = \dfrac{p_k}{q_k}$.

Theorem 4.6

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$$

Proof outline: By induction on k. □

Corollary 4.7 *For $1 \leq k \leq n$, p_k and q_k are relatively prime, i.e. $gcd(p_k, q_k) = 1$.*

Proof outline: If $d = gcd(p_k, q_k)$ then $d | p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$. But since $d \geq 1$, it implies that $d = 1$. □

Lemma 4.2 *$q_{k-1} \leq q_k$ for $1 \leq k \leq n$ and whenever $k > 1$, $q_{k-1} < q_k$.*

Theorem 4.8 *The convergents of an SFCF satisfy the following properties.*

1. *The even-indexed convergents form an increasing chain, i.e. $C_0 < C_2 < C_4 < \ldots$*
2. *The odd-indexed convergents form a decreasing chain, i.e. $C_1 > C_3 > C_5 > \ldots$*
3. *Every even-indexed convergent is smaller than every odd-indexed convergent.*

Proof outline: Consider $C_{k+2} - C_k = (C_{k+2} - C_{k+1}) + (C_{k+1} - C_k)$. Show that $sgn(C_{k+2} - C_k) = (-1)^k$. The first two parts then follow from this. To show the last part notice that for any j, we may first show again $C_{2j} < C_{2j-1}$ and $C_{2j+1} > C_{2j}$. Then for any i, j we have

$$C_0 < C_2 < \ldots C_{2j} < C_{2j+2i} < C_{2j+2i-1} < C_{2i-1} < \ldots < C_1$$

□

Algorithm 4.1 The Simple Continued Fraction Algorithm

```
algorithm scfa (x)
begin
    i := 0; x[0] := x; a[0] := floor(x[0]);
    print (a[0]);
    while (x[i] <> a[i]) do
    begin
        x[i+1] := 1/(x[i] - a[i]);
        a[i+1] := floor(x[i+1]);
        print (a[i+1]); i := i+1
    end
end.
```

Theorem 4.9 *Agorithm* `scfa`(x) *returns a finite list* $[a_0; a_1, a_2, \ldots, a_n]$ *if and only if* x *is rational, in which case* $x = [a_0; a_1, a_2, \ldots, a_n]$.

Proof outline: ($\Rightarrow$) If $[a_0; a_1, a_2, \ldots, a_n]$ is returned by the algorithm, it is easy to show by induction on i that $x_0 = [a_0; a_1, a_2, \ldots, a_{i-1}, x_i]$, for each i. Then clearly $x = x_0$ is a rational number with the stipulated value.

($\Leftarrow$) Suppose x is a rational. Then starting with $a_0 = \lfloor x_0 \rfloor$ and $x_{i+1} = 1/(x_i - a_i)$ we have that each x_i is rational, say u_i/u_{i+1}. We then have

$$\begin{aligned} x_{i+1} &= \frac{1}{x_i - ai} \\ &= \frac{1}{u_i/u_{i+1} - \lfloor u_i/u_{i+1} \rfloor} \\ &= \frac{u_{i+1}}{u_i - u_{i+1}\lfloor u_i/u_{i+1} \rfloor} \\ &= \frac{u_{i+1}}{u_i \bmod u_{i+1}} \end{aligned}$$

The transformation that takes x_i to x_{i+1} maps the pair (u_i, u_{i+1}) to $(u_{i+1}, u_i \bmod u_{i+1})$ which is precisely the transformation of the euclidean algorithm (algorithm 2.1), which we know terminates on integer inputs, eventually (when $u_i/u_{i+1} = \lfloor u_i/u_{i+1} \rfloor$, which is the termination condition $x_i = a_i$ of this algorithm. □

Theorem 4.10 `scfa`$(a/b) = [a_0; a_1, a_2, \ldots, a_n]$ *iff* $E(a, b) = n$.

We know that the linear diophantine equation (10.1) $ax + by = c$ has a solution if and only if $gcd(a, b)|c$. Further we also know that if (x_0, y_0) is a particular solution then the set of all solutions is given by

$$x = x_0 + (b/d)t \qquad\qquad y = y_0 - (a/d)t$$

for $d = gcd(a, b)$ and all integer values of t.

It follows therefore that $ax + by = c$ admits solutions iff $(a/d)x + (b/d)y = c/d$ admits of solutions. It is also clear that $gcd(a/d, b/d) = 1$.

Lemma 4.3 *If* (x_0, y_0) *is a solution of the equation* $ax + by = 1$*, where* $gcd(a, b) = 1$*, then* (cx_0, cy_0) *is a solution of* $ax + by = c$

Theorem 4.11 *The equation $ax + by = 1$ has a solution*

$$\begin{array}{rclrcll} x &=& q_{n-1} & y &=& -p_{n-1} & \textit{if } n \textit{ is odd, and} \\ x &=& -q_{n-1} & y &=& p_{n-1} & \textit{if } n \textit{ is even} \end{array}$$

Proof outline: Let $a/b = [a_0; a_1, a_2, \ldots, a_n]$. then $C_{n-1} = p_{n-1}/q_{n-1}$ and $C_n = p_n/q_n = a/b$. Since $gcd(p_n, q_n) = 1 = gcd(a, b)$, it follows that $p_n = a$ and $q_n = b$. Further since $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$ we have $aq_{n-1} - bp_{n-1} = (-1)^{n-1}$, which yeilds the required solutions depending upon whether n is even or odd. □

Chapter 5

Simple Infinite Continued Fraction

Definition 5.1 *The expression*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

where $a_0, a_1, a_2, \ldots$ *is an infinite sequence s.t.* $a_0 \in \mathcal{Z}$ *and* $\forall i \geq 1 \quad a_i \in \mathcal{N}$ *is called a* **simple infinite continued fraction (SICF)***, denoted by the list* $[a_0; a_1, a_2, \ldots]$.

Theorem 5.1 *The convergent of the SICF satisfy the infinite chain of inequalities*
$C_0 < C_2 < C_4 < \ldots < C_n < \ldots < C_{2n+1} < \ldots < C_5 < C_3 < C_1$

Proof: Similar to $Theorem$ 4.8 □

Theorem 5.2 *The even and odd convergent of a SICF converges to same limit.*

Proof: From $Theorem$ 5.1 it is clear that $\{C_{2n}\}$ forms a bounded monotonicaly increasing sequence bounded by C_1 and $\{C_{2n+1}\}$ forms a bounded monotonically decreasing sequence bounded by C_0 and so both will be converges to limit, say α and α' respectively. Clearly,

$$\alpha - \alpha' < C_{2n+1} - C_2 n$$

From $Theorem$ 4.6 ,

$$0 \leq \mid \alpha - \alpha' \mid < \frac{1}{q_{2n} \cdot q_{2n+1}} < \frac{1}{q_{2n}^2}$$

proof follows from the fact that we can make $\frac{1}{q_{2n}^2}$ arbitrarily small as q_i increases without bound for large i. □

Definition 5.2 *The value of the SICF can be defined as the limit of the sequence of rational numbers* $C_n = [a_0; a_1, a_2, \ldots, a_n]$ *(*$n \geq 0$ *) i.e. the SICF* $[a_0; a_1, a_2, \ldots]$ *has the value* $\lim_{n\to\infty} C_n$.

Note : The existence of the limit in the above definition is direct from the $Theorem$ 5.1 , $Theorem$ 5.2 and from the fact that the subsequences of $\{C_n\}$, even and odd numbered convergents ,converge to same limit α and so $\{C_n\}$ will also converge to the limit α.

Example 5.1 *Find the value of the SICF* $[1, 1, 1, \ldots]$ *(Golden ratio).*
Sol : *say* $\phi = [1, 1, 1, \ldots]$ *and* $C_n = \underbrace{[1, 1, 1, \ldots, 1]}_{n+1 \text{ terms}}$
From above definition,

$$\begin{aligned} \phi &= \lim_{n\to\infty} C_n \\ &= 1 + \frac{1}{\lim_{n\to\infty} C_{n-1}} \\ &= 1 + \frac{1}{\phi} \\ \Rightarrow \phi &= \frac{1+\sqrt{5}}{2} \end{aligned}$$

As the other root of the quadratic equation $\phi^2 - \phi - 1 = 0$ *is negative.*

Definition 5.3 *A* **simple periodic continued fraction** *is denoted by list*

$$[a_0; a_1, \ldots, \overline{a_n, \ldots, a_{n+k-1}}]$$

where bar over $a_n, \ldots, a_{n+k-1}$ *represent that the block* $(a_n, \ldots, a_{n+k-1})$ *is in repetition. This block is called the period of expantion and the number of elements in the block is called length of the block.*

Theorem 5.3 *Every SICF represents an irrational number.*

Proof: Let $C = [a_0; a_1, a_2, \ldots]$ be a SICF and $\{C_n\}$ be a sequence of convergent. Clearly , for any successive convergents C_n and C_{n+1} , C lies in between C_n and C_{n+1}

$$\Rightarrow 0 < | C - C_n | < | C_{n+1} - C_n | = \tfrac{1}{q_n q_{n+1}}$$

let us assume limit of convergent is a rational number , say $\frac{a}{b}$ for $a, b \in \mathcal{Z}$ and $b > 0$

$$\begin{aligned} \Rightarrow \quad & 0 < \left| \frac{a}{b} - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}} \\ \Rightarrow \quad & 0 < | aq_n - bp_n | < \frac{b}{q_{n+1}} \end{aligned}$$

As b is constant and $\forall i\ q_i < q_{i+1}$ (Lemma 4.2)

$$\begin{aligned} \Rightarrow \quad & \exists N \in \mathcal{N} \ s.t. \ \forall n \geq N, \ \frac{b}{q_{n+1}} < 1 \\ \Rightarrow \quad & 0 < | aq_n - bp_n | < 1, \ \ \forall n \geq N \end{aligned}$$

This is a contradiction as $| aq_n - bp_n | \in \mathcal{N}$, lies between 0 and 1 . □

Theorem 5.4 *If* $x = [a_0; a_1, a_2, \ldots] = [b_0; b_1, b_2, \ldots]$ *then* $a_n = b_n \forall n \geq 0$

Proof: Since $C_0 < x < C_1$ and $a_1, b_1 \in \mathcal{N}$

$$a_0 < x < a_0 + \frac{1}{a_1} \Rightarrow a_0 < x < a_0 + 1$$
$$b_0 < x < b_0 + \frac{1}{b_1} \Rightarrow b_0 < x < b_0 + 1$$

This implies that $a_0 = b_0$, since the greatest integer of x from one inequality is a_0 and from other is b_0 . Proof follows from the repetition of the argument on $[a_{k+1}, a_{k+2}, \ldots]$ and $[b_{k+1}, b_{k+2}, \ldots]$ by assuming that $a_i = b_i \; for \; 0 \leq i \leq k$ □

Corollary 5.5 *Distinct continued fractions represent distinct irrationals.*

Note : *Theorem* 5.3 and *Theorem* 5.4 together say that every SICF represents a unique irrational number.

Theorem 5.6 *Any irrational number x can be written as* $[a_0; a_1, a_2, \ldots, a_{n-1}, x_n]$, *where* a_0 *is a integer* ,$\forall i \; a_i \in \mathcal{N}$ *and for all n* x_n *is irrational.*

Proof outline: By induction on n. □

Theorem 5.7 *If* $x = [a_0; a_1, a_2, \ldots, a_{n-1}, x_n]$, *s.t.* $\forall n \geq 2 \; x_n \in \mathcal{R}_+$, $a_0 \in \mathcal{Z}$ *and* $\forall i \; a_i \in \mathcal{N}$ *then*

$$x = \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}}$$

Proof: (By induction on n) For $n = 2$,

$$x = [a_0; a_1, x_2] = \frac{x_2(a_0 a_1 + 1) + a_0}{x_2 a_1 + 1} = \frac{x_2 p_1 + p_0}{x_2 q_1 + q_0}$$

,the result is true. Assume the result hold for $n = k$ .i.e

$$[a_0; a_1, \ldots, a_{k-1}, x_k] = \frac{x_k p_{k-1} + p_{k-2}}{x_k q_{k-1} + qk - 2}$$

For $n = k + 1$, replace x_k by $a_k + \frac{1}{x_{k+1}}$

$$\begin{aligned} \Rightarrow x &= [a_0; a_1, \ldots, a_{k-1}, a_k + \frac{1}{x_{k+1}}] \\ &= \frac{(a_k + \frac{1}{x_{k+1}}) + p_{k-2}}{(a_k + \frac{1}{x_{k+1}}) + q_{k-1}} \\ &= \frac{x_{k+1} p_k + p_{k-1}}{x_{k+1} q_k + q_{k-1}} \end{aligned}$$

and so the result hold for all n. □

Corollary 5.8 *If* $x_m(n) = [a_m, a_{m+1}, \ldots, a_{n-1}, x_n]$, $m < n$ *and* $\lim_{n \to \infty} x_m(n) = y_m$, *then for* $m \geq 2$,

$$\begin{aligned} x = [a_0; a_1, a_2 \ldots] &= [a_0, a_1, \ldots, a_{m-1}, y_m] \\ &= \frac{y_m p_{m-1} + p_{m-2}}{y_m q_{m-1} q_{m-2}} \end{aligned}$$

Proof: Let m be fixed integer. Then by definition,

$$\begin{aligned} x &= lim_{n\to\infty}[a_0; a_1, \ldots, a_{m-1}[a_m, a_{m+1}, \ldots, a_n]] \\ &= lim_{n\to\infty}[a_0; a_1, \ldots, a_{m-1}, x_m(n)] \end{aligned}$$

Since $f(\alpha) = [a_0; a_1, \ldots, a_{m-1}, \alpha]$ is contineous function ,

$$\begin{aligned} \Rightarrow x &= [a_0; a_1, \ldots, a_{m-1}, lim_{n\to\infty}x_m(n)] \\ &= [a_0; a_1, \ldots, y_m] \end{aligned}$$

now result holds from $Theorem$ 5.6 for $m \geq 2$. □

Theorem 5.9 *For any irrational x ,*

$$\mid x - C_{n-1} \mid = \frac{1}{q_n q_{n-1}}$$

Proof: From $Theorem$ 5.6,

$$\begin{aligned} x - C_{n-1} &= \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_n - 2} - \frac{p_{n-1}}{q_{n-1}} \\ &= \frac{(-1)^{n-1}}{(x_n q_{n-1} + q_{n-2})q_{n-1}} \end{aligned}$$

Since $x_n > a_n$,

$$\begin{aligned} \mid x - C_{n-1} \mid &= \frac{1}{(x_n q_{n-1} + q_{n-2})q_{n-1}} \\ &< \frac{1}{(a_n q_{n-1} + q_{n-2})q_{n-1}} \\ &= \frac{1}{q_n q_{n-1}} \end{aligned}$$

□

Lemma 5.1 *If $x > 1$ and $x + \frac{1}{x} < \sqrt{5}$ then $x < \alpha$ $(= \frac{\sqrt{5}+1}{2})$ and $\frac{1}{x} = -\beta$ $(= \frac{\sqrt{5}-1}{2})$*
Sol : For $x > 1$, function $x + \frac{1}{x}$ increases without bounds. Given,

$$\begin{aligned} x + \frac{1}{x} &< \sqrt{5} \\ \Rightarrow (x - \alpha)(x - \beta) &< 0 \end{aligned}$$

This implies, either $x > \alpha$ and $x < -\beta$ or $x < \alpha$ and $x > -\beta$.Since $\alpha > -\beta$, so only second relation will hold . Now ,

$$\begin{aligned} x &< \alpha \\ \Rightarrow \frac{1}{x} &> \frac{2}{\sqrt{5}+1} = \frac{\sqrt{5}-1}{2} = -\beta \end{aligned}$$

Theorem 5.10 *Every irrational number can be uniquely represent as a SICF.Equivalently,*
If x is an irrational number , $a_0 = [x]$ and $a_k = [x_{k-1}]$ for $k = 1, 2 \ldots,$ where $x = a_0 + \frac{1}{x_0}$ and $x_i = a_{i+1} + \frac{1}{x_{i+1}}$ for $i = 0, 1, 2, \ldots$ then $x = [a_0; a_1, a_2, \ldots]$

Proof: The first n convergents of $[a_0; a_1, \ldots]$ are same as the first n convergents of $[a_0; a_1, \ldots, a_n.x_n]$.Thus $n+1^{th}$ convergent of $[a_0; a_1, \ldots, a_n, x_n]$ from *Theorem* 5.6 is

$$x = \frac{x_n p_n + p_{n-1}}{x_n q_n + q_{n-1}}$$

however ,

$$x - C_n = \frac{(-1)^{n+1}}{(x_n q_n + q_{n-1})q_n}$$

For $n > 1,\ n-1 \leq (n-1)^2 \leq q_n^2 < (x_n q_n + q_{n-1})q_n$, this implies that the denominator becomes infinite as n increases and so ,

$$x - \lim_{n\to\infty} C_n = lim_{n\to\infty}(x - C_n) = 0$$

hence , every irrational number uniquely represents an infinite simple continued fraction.(uniqueness follows from Theorem 5.4) □

Corollary 5.11 *For any irrational number x ,*

$$\mid x - \frac{p_n}{q_n} \mid < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}$$

where $C_n = \frac{p_n}{q_n}$ *is* n^{th} *convergent.*

Example 5.2 *Prove that e is an irrational number.*
Sol : *Proof by contradiction,*
Assume that $e = \frac{a}{b},\ a > b > 0$ *is an rational number.Then for* $n > b$ *and also* $n > 1$ *,*

$$\begin{aligned} N &= n!\,(\,e - \sum_{k=0}^{n} \frac{1}{k!}\,) \\ &= n!\,(\,\sum_{k>n} \frac{1}{k!}\,) \end{aligned}$$

since , $e = \sum_{n\geq 0} \frac{1}{n!}$. *Also note that the number N is a positive integer,*

$$\begin{aligned} \Rightarrow N &= \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} + \ldots \\ &< \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \frac{1}{(n+2)(n+3)} + \ldots \\ &= \frac{2}{n+1} < 1 \end{aligned}$$

since $n > 1$ *. This is a contradiction as n is a positive integer. This implies that e must be a irrational.*

Theorem 5.12 *For any irrational number* $x > 1$ *, the* $n+1^{th}$ *convergent of* $\frac{1}{x}$ *and the* n^{th} *convergent of x are reciprocal to each other.*

Proof outline: Let $x = [a_0, a_1, a_2, \ldots]$. Now proof follows from the observation,

$$\begin{aligned} \frac{1}{x} &= 0 + \frac{1}{[a_0, a_1, a_2 \ldots]} \\ &= \lim_{n\to\infty} (0 + \frac{1}{[a_0, a_1, \ldots, a_n]}) \\ &= \lim_{n\to\infty} [a, a_0, a_1, \ldots, a_n] \\ &= [0, a_0, a_1, \ldots] \end{aligned}$$

□

Corollary 5.13 *For any irrational x in between 0 and 1 , the $n+1^{th}$ covergent of x and n^{th} convergent of 1/x are reciprocal to each other.*

Chapter 6

Rational Approximation of Irrationals

In this chapter we consider the problem of finding good rational approximations to an irrational number x.

Definition 6.1 *The* best approximation *to a real number x relative to n is the rational number p/q closest to x such that $0 < b \leq n$.*

The next theorem shows that continued fraction convergents are the best approximations relative to their denominators.

Lemma 6.1 *Let $c_n = \frac{p_n}{q_n}$ be the n^{th} convergent of* SICF *representation of x. If $a, b \in \mathbb{Z}$ with $1 \leq b \leq q_{n+1}$, then $| q_n x - p_n | \leq | bx - a |$*

Proof: Consider the equation

$$\begin{bmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{bmatrix} \begin{bmatrix} y \\ z \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$$

Note that

$$\begin{vmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{vmatrix} = (-1)^{n+1}$$

So, the equation has unique integer solutions given by

$$\begin{aligned} y_o &= (-1)^{n+1}(aq_{n+1} - bp_{n+1}) \\ z_o &= (-1)^{n+1}(bp_n - aq_n) \end{aligned}$$

<u>Claim.$y_o \neq 0$</u>
If $y_o = 0$ then $aq_{n+1} = bp_{n+1}$. We know that $\gcd(p_{n+1}, q_{n+1}) = 1$. The two facts imply $q_{n+1} \mid b$ which in turn implies $b \geq q_{n+1}$, which is a contradiction.

We now consider two cases depending on value of z_o:
<u>Case:</u> $z_o = 0$
$\Rightarrow bp_o = aq_n$ and since $y_o \in \mathbb{Z}$, $| q_n x - p_n | \leq | bx - a |$. Hence proved.

<u>Case:</u> $z_o \neq 0$
<u>Claim.$y_o z_o < 0$</u>
If $z_o < 0$ then $y_o q_n + z_o q_{n+1} = b \Rightarrow y_o q_n = b - z_o q_{n+1} > 0 \Rightarrow y_o > 0$.
If $z_o \geq 0$ then, $b < q_{n+1} \Rightarrow y_o q_n = b - z_o q_{n+1} < 0 \Rightarrow y_o < 0$.

As x lies between $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$, $(x-\frac{p_n}{q_n})$ and $(x-\frac{p_{n+1}}{q_{n+1}})$ have opposite signs.Hence (q_nx-p_n) and $(q_{n+1}x-p_{n+1})$ have opposite signs.

$$\begin{aligned} p_ny_o + p_{n+1}z_o &= a \\ q_ny_o + q_{n+1}z_o &= b \end{aligned}$$

$$\begin{aligned} \mid bx-a \mid &= \mid y_o(q_nx-p_n) + z_o(q_{n+1}x-p_{n+1}) \mid \\ &= \mid y_o \mid \mid q_nx-p_n \mid + \mid z_o \mid \mid q_{n+1}x-p_{n+1} \mid \\ &\geq \mid q_nx-p_n \mid \end{aligned}$$

where the second equality follows because $\mid a+b \mid = \mid a \mid + \mid b \mid$ if a and b have same signs.

□

Theorem 6.1 *If* $1 \leq b \leq q_n$ *then* $\mid x - \frac{p_n}{q_n} \mid \leq \mid x - \frac{a}{b} \mid$

Proof: Assume the statement is false.

$$\begin{aligned} \mid q_nx-p_n \mid &= q_n \mid x - \frac{p_n}{q_n} \mid \\ &> b \quad \mid x - \frac{a}{b} \mid \\ &= \quad \mid bx-a \mid \end{aligned}$$

which contradicts the previous lemma. □

Hence continued fraction convergents are the best approximations to irrationals relative to their denominators.

Theorem 6.2 *If* $x = [a_0, a_1 \ldots a_{n-1}, x_n], x_n \in \mathbb{R}^+$ *for all* $n \geq 0$ *then* $x = \frac{x_np_{n-1}+p_{n-2}}{x_nq_{n-1}+q_{n-2}}$

Proof: By induction on n.
*Base:*For $n = 2$,

$$\begin{aligned} x = [a_0; a_1, x_2] &= \frac{x_2(a_0a_1+1)+a_0}{x_2a_1+1} \\ &= \frac{x_2p_1+p_0}{x_2q_1+q_0} \end{aligned}$$

I.H. Assume the result holds for $n = k$ .i.e

$$[a_0; a_1, \ldots, a_{k-1}, x_k] = \frac{x_kp_{k-1}+p_{k-2}}{x_kq_{k-1}+qk-2}$$

For $n = k+1$, replace x_k by $a_k + \frac{1}{x_{k+1}}$

$$\begin{aligned} \Rightarrow x &= [a_0; a_1, \ldots, a_{k-1}, a_k + \frac{1}{x_{k+1}}] \\ &= \frac{(a_k + \frac{1}{x_{k+1}}) + p_{k-2}}{(a_k + \frac{1}{x_{k+1}}) + q_{k-1}} \\ &= \frac{x_{k+1}p_k + p_{k-1}}{x_{k+1}q_k + q_{k-1}} \end{aligned}$$

and so the result holds for all n. □

Lemma 6.2 *If $x > 1$ and $x + 1/x < \sqrt{5}$ then*

i. $x < \alpha = \frac{\sqrt{5}+1}{2}$

ii. $\frac{1}{x} > -\beta = \frac{\sqrt{5}-1}{2}$

Proof: Note that α and β are roots of equation $x + 1/x = \sqrt{5}$.

$$x + 1/x < \sqrt{5} \Rightarrow (x - \alpha)(x - \beta) < 0$$

The two possibilities are $\alpha < x < -\beta)$ *or* $-\beta < x < \alpha$. The first one is ruled out as we are given that $x > 1 > -\beta$. So, we have $-\beta < x < \alpha$ which proves the first claim.
Now, $x < \alpha \Rightarrow x < \frac{\sqrt{5}+1}{2} \Rightarrow \frac{1}{x} > \frac{2}{\sqrt{5}+1} = \frac{\sqrt{5}-1}{2}$ which proves the second claim. □

Theorem 6.3 Hurwitz's Theorem *Given an irrational x, there exist many rationals a/b such that*

$$| x - \frac{a}{b} | < \frac{1}{\sqrt{5}b^2} \tag{6.1}$$

Proof: We first prove certain claims
Claim. If 6.1 is false for any consecutive C_{n-1} and C_n, then $r_n + 1/r_n < \sqrt{5}$ where $r_n = q_n/q_{n-1}$.
We are given $| x - \frac{p_{n-1}}{q_{n-1}} | \geq \frac{1}{\sqrt{5}q_{n-1}^2}$ and $| x - \frac{p_n}{q_n} | \geq \frac{1}{\sqrt{5}q_n^2}$. So, $| x - C_{n-1} | + | x - C_n | \geq \frac{1}{\sqrt{5}}(\frac{1}{q_n^2} + \frac{1}{q_{n-1}^2})$. Since x lies between C_{n-1} and C_n, $| x - C_{n-1} | + | x - C_n | = | \frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} | = \frac{1}{q_{n-1}q_n}$. Hence,

$$\begin{aligned}
\frac{1}{q_{n-1}q_n} &\geq \frac{1}{\sqrt{5}}(\frac{1}{q_n^2} + \frac{1}{q_{n-1}^2}) \\
\Rightarrow \frac{q_n}{q_{n-1}} &\geq \frac{1}{\sqrt{5}}(\frac{q_n^2}{q_{n-1}^2} + 1) \\
\Rightarrow r_n &\geq \frac{1}{\sqrt{5}}(r_n^2 + 1) \\
\Rightarrow r_n + 1/r_n &\leq \sqrt{5}
\end{aligned}$$

Claim. Atleast one of three consecutive convergents satisfies 6.1
Assume none of C_{n-1}, C_n and C_{n+1} satisfy 6.1. Using the previous claim, $r_n + 1/r_n < \sqrt{5}$. But by lemma 6.2 $r_n < \alpha$ and $1/r_n > -\beta$. Similarly, $r_{n+1} < \alpha$ and $1/r_{n+1} > -\beta$.

$$\begin{aligned}
q_{n+1} &= a_n q_n + q_{n-1} \\
\Rightarrow r_{n+1} &= a_n + \frac{1}{r_n} \\
&< \alpha_n + \frac{\sqrt{5}-1}{2} \\
&< \frac{\sqrt{5}+1}{2}
\end{aligned} \tag{6.2}$$

where the last inequality follows since $r_{n+1} < \alpha$. Combining the last two inequalities, we get $a_n < 1$, which is a contradiction and the claim is proved.

Since an irrational has infinite convergents, *Hurwitz's theorem* follows from the claim. □

Theorem 6.4 *For any constant $c > \sqrt{5}$* , Hurwitz's theorem *does not hold.*

Proof: Consider the irrational number $\alpha = [1, 1\ldots]$. There exists $n \geq 0$ such that, $\alpha_n = \alpha$,$p_n = F_n$ and $q_n = F_{n-1}$.

$$\lim_{n \to \inf} (\frac{q_n}{q_{n+1}}) = \lim_{n \to \inf} (\frac{q_n}{p_n}) = \frac{1}{\alpha} = -\beta$$

$$\begin{aligned} \mid \alpha - \frac{p_n}{q_n} \mid &= \frac{1}{q_{n-1}(\alpha_n q_{n-1} + q_{n-2})} \\ &= \frac{1}{q_n^2(\alpha_{n+1} + \frac{q_{n-1}}{q_n})} \end{aligned}$$

Consider the term $\alpha_{n+1} + \frac{q_{n-1}}{q_n}$.

$$\begin{aligned} \lim_{n \to \inf} & \quad \alpha_{n+1} + \tfrac{q_{n-1}}{q_n} \\ &= \alpha + -\beta = \sqrt{5} \end{aligned}$$

So, for any $c > \sqrt{5}, \alpha_{n+1} + \frac{q_{n-1}}{q_n} > c$ for only a finite number of n's. We have shown that if $\mid x - \frac{a}{b} \mid < \frac{1}{2b^2}$ then $\frac{a}{b}$ is a convergent.Now,

$$\begin{aligned} \mid \alpha - \frac{p_n}{q_n} \mid &= \frac{1}{q_n^2(\alpha_{n+1} + \frac{q_{n-1}}{q_n})} \\ &< \frac{1}{cq_n^2} \\ &< \frac{1}{2q_n^2} \end{aligned}$$

where the first inequality holds only for a finite number of convergents and the second inequality holds only for rationals which are convergents. Hence there are only a finite number of rationals of the form $\frac{a}{b}$ such that $\mid \alpha - \frac{a}{b} < \frac{1}{cb^2}$ for $c > \sqrt{5}$. □

Chapter 7

Quadratic Irrational(Periodic Continued Fraction)

Definition 7.1 *An element* $x \in R$ *is a quadratic irrational if it is irrational and satisfies a quadratic polynomial.*
Thus, e.g., $(1+\sqrt{5})/2$ *is a quadratic irrational. Recall that*

$$\frac{1+\sqrt{5}}{2} = [1,1,1,\ldots]$$

Definition 7.2 *A periodic continued fraction is a continued fraction* $[a_0, a_1, \ldots, a_n, \ldots]$ *such that.*

$$a_n = a_{n+h}$$

for a fixed positive integer h *and all sufficiently large* n*. We call* h *the period of the continued fraction.*

Example 7.1 *Consider the periodic continued fraction* $[1,2,1,2,\ldots] = [\overline{1,2}]$.

$$[\overline{1,2}] = 1 + \frac{1}{2 + \frac{1}{1+\frac{1}{2+\frac{1}{1+\cdots}}}},$$

Lemma 7.1 *1) A periodic continued fraction represent a quadratic irrationals.*
2) Any quadratic irrational has SPCF representation.

Theorem 7.1 *Every quadratic irrational has SPCF representation.*
Proof Outline : *Let say that* x *is a quadratic irrational.*

$$x = \frac{b+\sqrt{d}}{c}$$

where $b, d, c \in \mathbb{Z}$ *but* d *is squarefree integer.*
let say

$$x = \frac{m+\sqrt{d}}{s_0} \qquad \text{where } s_0|(d-m^2)$$

$$a_i = [x_i] \qquad x_i = \frac{m_i+\sqrt{d}}{s_i}$$
$$m_{i+1} = a_i s_i - m_i$$
$$s_{i+1} = \frac{d-m_{i+1}^2}{s_i}$$

Claim : *m_i, s_i are all integers.*
Proof : *By induction on i.*
Base Case : m_0 and s_0 are b and c and $b, c \in \mathbb{Z}$
Let say it is true for i. m_i, s_i are integers and $s_i|(d-m_{i+1}^2)$.
then

$$s_{i+1} = \frac{d-m_{i+1}^2}{s_i} = \frac{d-(a_i s_i - m_i)^2}{s_i}$$
$$\Rightarrow \frac{d-m_i^2}{s_i} + 2a_i m_i - a_i^2 s_i$$
$$\Rightarrow s_{i+1} \text{ is an integer and } s_{i+1} = 0$$

because otherwise $d = m_{i+1}^2$ contractiong the property of d.
Claim : *x is a periodic .*
Proof : *say $\overline{x} = \frac{m_i-\sqrt{d}}{s_i}$ since the conjugate of quotients equals quotients of conjugates.*

$$x = \frac{x_n p_{n-1}+p_{n-2}}{x_n q_{n-1}+q_{n-2}}$$

for any $x > 0$

$$p_k = q_k p_{k-1} + p_{n-2}$$
$$p_k = o_k q_{k-1} + q_{n-2}$$

for all $k \geq 0$

$$\overline{x} = \frac{\overline{x_n} p_{n-1}+p_{n-2}}{\overline{x_n} q_{n-1}+q_{n-2}}$$

manipulate it.

$$\begin{aligned} \overline{x_n} &= -(\frac{\overline{x}q_{n-2}+p_{n-2}}{\overline{x}q_{n-1}+p_{n-1}}) \\ &= -\frac{q_{n-2}}{q_{n-1}}(\frac{\overline{x}-\frac{p_{n-2}}{q_{n-2}}}{\overline{x}-\frac{p_{n-1}}{q_{n-1}}}) \\ \Rightarrow \overline{x_n} &= -\frac{q_{n-2}}{q_{n-1}}(\frac{\overline{x}-\frac{p_{n-2}}{q_{n-2}}}{\overline{x}-\frac{p_{n-1}}{q_{n-1}}}) < 0 \end{aligned}$$

because

$$\lim_{n\to\infty} \frac{p_{n-1}}{q_{n-1}} = x$$

$\overline{x} < 0$ for sufficiently s.t.

$$x_n > 0$$

where

$$x_n = \frac{m+\sqrt{d}}{s_n}, \qquad \overline{x_n} = \frac{m-\sqrt{d}}{s_n}$$
$$x_n - \overline{x_n} = \frac{2\sqrt{d}}{s_i} > 0$$
$$\Rightarrow s_n > 0 \qquad similarly \quad s_{n+1} > 0$$
$$s_n.s_{n+1} = d - m_{n+1}^2 \leq d$$
$$s_n \geq s_n.s_{n+1} \leq d$$
$$m_{n+1}^2 < m_{n+1}^2 + s_n.s_{n+1} < d$$
$$\Rightarrow 0 \leq |m_{n+1}| < \sqrt{d}$$
$$m_i = m_j \qquad forall \quad j < k$$

so that

$$s_j = s_k$$

and

$$x = [a_0, \ldots, a_{j-1}, \overline{a_j, \ldots, a_{k-1}}]$$

so every quadratic irrationals has SPCF representation

Theorem 7.2 *Every SPCF has quadratic representation.*
Proof : *First suppose that*

$$[a_0, a_1, \ldots, a_n, \overline{a_{n+1}, \ldots, a_{n+k}}]$$

is a periodic continued fraction. Set $\alpha = [a_{n+1}, a_{n+2}, \ldots]$. *Then*

$$\alpha = [a_{n+1}, \ldots, a_{n+k}, \alpha],$$

so

$$\alpha = \tfrac{\alpha p_{n+k} + p_{n+k-1}}{\alpha q_{n+k} + q_{n+k-1}}.$$

(We use that α *is the last partial convergent.) Thus* α *satisfies a quadratic equation. Since the* a_i *are all integers, the number*

$$\begin{aligned}[a_0, a_1, \ldots] &= [a_0, a_1, \ldots, a_n, \alpha] \\ &= a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots + \alpha}}\end{aligned}$$

can be expressed as a polynomial in α *with rational coefficients, so* $[a_0, a_1, \ldots]$ *also satisfies a quadratic polynomial. Finally,* $\alpha \notin \mathbb{Q}$ *because periodic continued fractions have infinitely many terms.*

Theorem 7.3 *The CF expansions of a qudratic irrationals x is purely periodic iff* $x > 1$ *and* $-1 \leq \overline{x} < 0$
Proof : ($\Longleftarrow$) *Assume* $x > 1$ *and* $-1 \leq \overline{x} < 0$

$$x_{i+1} = \frac{1}{x_i - a_i} \quad ; \quad \frac{1}{x_{i+1}} = x_i - a_i$$

as

$$x = [a_0, \ldots]$$

so

$$x > 1 \quad \Rightarrow \quad a_0 \geq 1 \quad a_i \geq 1 \quad \forall i > 0$$
$$x > 1 \quad and \quad a_0 \geq 1 \Rightarrow \frac{1}{\overline{x_{i+1}}} = \overline{x_i} - a_i < -1$$

By induction : let say

$$-1 < \overline{x} < 0$$
$$\Rightarrow -1 < \frac{1}{\overline{x_{i+1}}} < 0$$
$$\Rightarrow a_i = -\frac{1}{\overline{x_{i+1}}}$$

x is quadratic irrationals and hence is periodic

$\exists j > i \quad a_i = a_j$ *and* $x_i = x_j$
so $\overline{x_i} = \overline{x_j}$

$$a_{j-1} = -\frac{1}{\overline{x_j}} = -\frac{1}{\overline{x_i}} = a_{i-1}$$

Proof : ($\Longrightarrow$) *Assume*

$$x = [a_0, \overline{a_1, \ldots, a_{n-1}}]$$
$$x = [a_0, a_1, \ldots, a_{n-1}, x]$$
$$x = \frac{xp_{n-1} + p_{n-2}}{xq_{n-1} + q_{n-2}}$$
$$F(x) = x^2 q_{n-1} + x(q_{n-2} - p_{n-1} - p_{n-2}$$

there won't be any imaginary roots for this equation

Two roots α *and* β ,
$a_0 > 1, x \geq 1$ $a_0 = a_n \Rightarrow a_n > 0 \Rightarrow a_0 = 0$
$a_0, \ldots, a_{n-1}$ *are all the one of* $\alpha, \overline{\alpha} > 1$
To proove that $-1 < \alpha < 0$
Claim : *$F(-1)$ and $F(0)$ have opposite sign.*

$$F(0) = p_{n-2} < 0$$
$$F(-1) = q_{n-1} - q_{n-2} + p_{n-2} - p_{n-1} > 0$$

for $n > 1$

Chapter 8

Primes and ther Infinitude

It will be another million years, at least, before we understand the primes. - P. Erdös

For any integer $m \in \mathbb{Z}^+$, define $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ as the set of positive integers less than m. Consider a relation $\equiv_m \subset \mathbb{Z}^+ \times \mathbb{Z}^+$, where $a \equiv_m b$ if and only if $m \mid (a - b)$.

$\equiv_m$ is an equivalence relation

- **Reflexive:** $a \equiv_m a$, for all $a \in \mathbb{Z}^+$.
- **Symmetric:** If $a \equiv_m b$, then $a - b = k_1 m$. So $b - a = -k_1 m$, and $b \equiv_m a$.
- **Transitive:** If $a \equiv_m b$ (implying that $a - b = k_1 m$) and $b \equiv_m c$ (implying that $b - c = k_2 m$), then $a - c = (k_1 + k_2)m$, and hence $a \equiv_m c$.

Therefore, we can partition the set of integers into m equivalence classes, corresponding to the remainder the number leaves when divided by m. Therefore, any integer $a \in \mathbb{Z}$ is mapped to a number $r \in \mathbb{Z}_m$, where $a \equiv_m r$. Let $[a]$ denote the remainder of a when divided by m. Therefore, $a \equiv_m [a]$, where $[a] < m$.

The equivalence relation is preserved under addition (+), subtraction (−) and multiplication (×). Let $a = q_a m + r_a$, with $0 \leq r_a < m$, and $b = q_b m + r_b$ with $0 \geq r_b < m$. Then $[a] = r_a$ and $[b] = r_b$. Therefore $[a] \circ [b] = r_a \circ r_b$, where $\circ \in \{+, -, \times\}$.

- $[a] +_m [b] = [a + b]$. $[a + b] = [q_a m + r_a + q_b m + r_b] = [(q_a + q_b)m + (r_a + r_b)] = [r_a + r_b] = [a] + [b]$.
- $[a] -_m [b] = [a - b]$. $[a - b] = [q_a m + r_a - q_b m - r_b] = [(q_a - q_b)m + (r_a - r_b)] = [r_a - r_b] = [a] - [b]$.
- $[a] \times_m [b] = [a \times b]. [a \times b] = [(q_a m + r_a) \times (q_b m + r_b)] = [q_a q_b m^2 + (r_b q_a + r_a q_b)m + r_a r_b] = [r_a r_b] = [a] \times [b]$.

Multiplicative Inverse We say $b \in \mathbb{Z}_m$ is the multiplicative inverse of a if

$$ab \equiv_m 1$$

Theorem 8.1 *The elements of $\mathbb{Z}_m$ which have multiplicative inverses are exactly those that are relatively prime to m.*

Proof: By definition, b is a multiplicative inverse of a if and only if $ab \equiv_m 1$. Therefore, $ab = qm + 1 \Rightarrow ab - mq = 1$. Recall from linear diaphantine equations that $ax + by = c$ has a solution if and only if $gcd(a, b) \mid c$. Therefore, for the multiplicative inverse b to exist, we require that $gcd(a, m) \mid 1 \Rightarrow gcd(a, m) = 1$. Therefore, if a has a multiplicative inverse, then it must be relatively prime to m. □

Corollary 8.2 *For every prime number p, every non-zero element in $\mathbb{Z}_p$ has a multiplicative inverse.*

Recall that a *group* is defined as a set S, together with a binary operation $S \times S \rightarrow S$, satisfying the following axioms (where we write $a * b$ for the result of applying the binary operation to the two elements $a, b \in S$.)

- *associativity*: for all a, b and c in S, $(a * b) * c = a * (b * c)$.
- *identity element*: there is an element e in S such that for all a in S, $e * a = a = a * e$.
- *inverse element*: for all a in S there is a b in S such that $a * b = e = b * a$.

A *group* whose operation is commutative (that is, $a * b = b * a$ for all $a, b \in S$ is also called a *Abelian* or *commutative* group. Let $[\mathbb{Z}_p, +_p, 0]$ define a *abelian* group, where $\mathbb{Z}_p$ is the set, and the binary operation is the addition operation modulo p ($+_p$). For all a, b and c in S, $(a +_p b) +_p c = a +_p (b +_p c)$. Further, $0 \in \mathbb{Z}_p$ is the identity element since for all $a \in \mathbb{Z}_p$, $a +_p 0 = a = 0 +_p a$. Finally, there exists an inverse element for every element $a \in \mathbb{Z}_p = p - a$.

$[\mathbb{Z}_p, \times_p, 1]$ is also an *abelian* group. For associativity, we require that for all a, b and c in $\mathbb{Z}_p$, we have $(a \times_p b) \times_p c = a \times_p (b \times_p c)$. If $a = q_a \cdot p + r_a$, $b = q_b \cdot p + r_b$ and $c = q_c \cdot p + r_c$, with $0 \leq r_a,\ r_b,\ r_c < p$, then $a \times b = q_a q_b p^2 + (q_a + q_b)p + r_a r_b$. Therefore, $a \times_p b = r_a r_b \ mod\, p$, which means that $(a \times_p b) \times_p c = r_a r_b r_c \ mod\ p$. Similary, we have $a \times_p (b \times_p c) = r_a r_b r_c \ mod\, p$. Further $1 \in \mathbb{Z}_p$ is the identity element since for all $a \in \mathbb{Z}_p$, $a \times_p 1 = a = 1 \times_p a$. Finally, there exists an inverse element for every element $a \in \mathbb{Z}_p$ by the corollary.

We know that a number $p > 1$ is a prime number if it has no non-trivial factors (other than 1 and p itself). The following are some simple observations about any prime number p.

1. $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.
2. $p \mid a_1 a_2 \ldots a_k \Rightarrow p \mid a_i$ for some $1 \leq i \leq k$.
3. $p \mid q_1 q_2 \ldots q_k \Rightarrow p = q_i$ for some $1 \leq i \leq k$, where $q_1, q_2, \ldots, q_k$ are all primes.

We are used to considering primes only on natural numbers. Here is another set of primes over a different set. Consider the set of all even numbers $\mathbb{Z}_e$. The set $\mathbb{Z}_e$ has the following properties:

- for all $a, b, c \in \mathbb{Z}_e$, $a + (b + c) = (a + b) + c$ - *associativity.*
- for all $a \in \mathbb{Z}_e$, there is an element $-a \in \mathbb{Z}_e$, such that $a + 0 = 0 + a = a$, and $0 \in \mathbb{Z}_e$ - *identity element.*

that this set forms an *abelian group* since it satisfies *associativity*, has an *identity element* (0), and for every even number $x \in \mathbb{Z}_e$, the negation $-e$ is the unique inverse element under the operation $+$. Therefore, we have a notion of primality over the *ring* of even numbers. The only primes in $\mathbb{Z}_e$ are the numbers of the form $2 \cdot (2k + 1)$, since they have no factorizations over $\mathbb{Z}_e$.

Theorem 8.3 Fundamental Theorem of Arithmetic *Every positive integer $n > 1$ is a product of prime numbers, and its factorization into primes is unique up to the order of the factors.*

Proof: *Existence:* By Induction. In the base case, $n = 2$ and $n = 3$ are both primes, and hence the theorem holds. Let us suppose that the hypothesis holds for all $m < n$. The number n is either prime, in which case the hypothesis holds $(1 \times n)$, or composite, in which case $n = ab$ with $a < n$ and $b < n$. Since both a and b are products of primes (by induction hypothesis) the theorem holds for n.

Uniqueness: Let us assume that n has two representations $n_1 = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, and $n_2 = q_1^{d_1} q_2^{d_2} \ldots q_k^{e_k}$. Without loss of generality, assume that $p_1 < p_2 < \ldots < p_k$ and that $q_1 < q_2 < \ldots < q_l$. Let $P = \{p_1, p_2, \ldots, p_k\}$ amd $Q = \{q_1, q_2, \ldots, q_l\}$. We will first prove that $P = Q$ (which implies that $l = k$ and $p_i = q_i$. We will then show that $e_i = d_i$ for $1 \leq i \leq k$, and that would imply that the two factorizations are identical, hence completing the proof of uniqueness.

Let us suppose that $P \neq Q$. Let $x \in P$ and $x \notin Q$. Then we have $x \mid n_1$. Since x is a prime, there is no $y \in Q$ such that $x \mid y$. Therefore, $x \nmid n_2$. But since $n_1 = n_2$, we arrive at a contradiction, so that if $x \in P$ then $x \in Q$. Similarly, by symmetry, we have if $x \in Q$ then $x \in P$. Hence $P = Q$, and therefore $p_i = q_i$.

Next, we will show that $e_i = d_i$ for all $1 \leq i \leq k$. Suppose $e_i \neq d_i$ for some $1 \leq i \leq k$. Let $c_i = \max(e_i, d_i)$. Once again, $p_i^{c_i} \mid n$ is one representation and not in the other. That is impossible, therefore $e_i = d_i$ for all $1 \leq i \leq k$. □

Theorem 8.4 *There are an infinite number of prime numbers.*

Proof: We present a proof by contradiction. Assume that there are a finite number m of primes which are $p_1, p_2, \ldots, p_m$. Consider the natural number $p = p_1 p_2 \ldots p_m + 1$. We have that $p \nmid p_i$ for $1 \leq i \leq m$. Since any number must have a unique prime factorization, and the prime factorization of p does not have p_i for $1 \leq i \leq m$, there must be some other primes that appear in its prime factorization. Therefore, we arrive at a contradiction and our initial assuption that there are only a finite number of primes does not hold. □

Corollary 8.5 *If p_i is the ith prime number, with $p_1 = 2$, we can claim that $p_{m+1} \leq p$ since there is a prime factor of p that is not covered in $p_1, p_2, \ldots, p_m$.*

Theorem 8.6 *If the p_n denotes the nth prime, then $p_n \leq 2^{2^{n-1}}$ (the first prime $p_1 = 2$).*

Proof: We present a proof by induction on n. *Induction Hypothesis:* For all $n \leq k$, if p_n denotes the nth prime, then $p_n \leq 2^{2^{n-1}}$. *Base Case:* If $n = 1$, then $p_n = 2$, and $2^{2^{n-1}} = 2^{2^0} = 2$, hence $2 \leq 2$. *Induction Case:* In the induction case, let us assume that the induction hypothesis holds for all $n \leq k$. Then:

$$\begin{aligned} p_{k+1} &\leq p_1 p_2 \ldots p_k + 1 && \textit{by Corollary 2} \\ &\leq 2^{2^0} 2^{2^1} \ldots 2^{2^{k-1}} + 1 && \textit{by IH} \\ &\leq 2^{2^0 + 2^1 \ldots + 2^{k-1}} \\ &\leq 2^{2^k - 1} + 1 && \textit{Summing up } 2^i \\ &\leq 2^{2^k} \end{aligned}$$

And that completes the proof. □

Corollary 8.7 *There are at least $n+1$ primes that are less than 2^{2^n}.*

Claim 8.1 *The product of any two terms of the form $4n+1$ is also of the form $4n+1$.*

Proof: Consider $n_1 = 4k_1+1$ and $n_2 = 4k_2+1$. Therefore $n_1n_2 = (4k_1+1)(4k_2+1) = 16k_1k_2+4(k_1+k_2)+1 = 4k+1$ with $k = 4k_1k_2 + (k_1 + k_2)$. □

Theorem 8.8 *There are an infinite number of primes of the form $4n + 3$.*

Proof: We present a proof by contradiction. Let us assume that $q_1, q_2, \ldots, q_k$ are the only primes that are of the form $4n + 3$. Consider the number N:

$$\begin{aligned} N &= 4\Pi_{i=1}^{k} q_i - 1 \\ &= 4(\Pi_{i=1}^{k} q_i - 1) + 3 \end{aligned}$$

Since N is odd, all its factors must be odd. Hence, all its factors are either of the form $4n + 1$ or $4n + 3$. Since the product of two numbers of the form $4n + 1$ is also a number of the form $4n + 1$ (from the previous claim), we require that N has at least one factor of the form $4n + 3$. Therefore, there exists a prime number r that is of the form $4n+3$ that is a factor of N. Further, no q_i is a factor of N. Therefore, N has a factor that is of the form $4n + 3$ other than the q_i for $1 \leq i \leq k$. But by our assumption q_i are the only prime numbers of the form $4n + 3$. This brings us to a contradiction and hence there are an infinite number of primes of the form $4n + 3$. □

Generalizing, we may wish to ask if there are any primes of a general form $a + ib$, where a and b are integers and i ranges over the naturals.

Theorem 8.9 *If the n terms of the arithmetic progression*

$$p, p + d, p + 2d, \ldots, p + (n - 1)d$$

are all prime numbers, then the common difference d is divisible by every prime $q < n$.

Proof: We present a proof by contradiction. Assume on the contrary that a prime number $q < n$ exists such that $q \nmid d$. Consider the set

$$S = \{p + id \mid 0 \leq i < q\}$$

Claim 8.2

$$S \equiv_q \{0, 1, \ldots, q - 1\}$$

Proof: (Of the claim) We will prove this using the fact that two different elements of the set S yield distinct remainders when divided by the prime q. Consider any two elements $e_1 = p + id \in S$ and $e_2 = p + jd \in S$. We have $e_1 - e_2 = (i - j)d$. Since $q \nmid d$ and $i - j < q \Rightarrow q \nmid i - j$, and q is prime, it follows that $q \nmid e_1 - e_2$. Therefore, e_1 and e_2 are not congruent modulo the prime p. □

Therefore, $|S| = q$, and there must exist an element $p + kd \in S$ such that $p + kd \equiv_q 0$. This brings us to a contradiction since all terms of the arithmetic progression are primes. Therefore, our assumption that $q \nmid d$ fails, and the proof is complete. □

Theorem 8.10 Dirichlet's Theorem: *If a and b are relatively prime (that is $gcd(a, b) = 1$), then there are infinite primes of the form $a + ib$, $i \in \{0, 1, \ldots, \}$.*

Remark 8.1 *Note that the requirement $gcd(a, b) = 1$ is crucial. If $gcd(a, b) = k$ with $k > 1$, then it is clear that $k \mid a + ib$. Since all numbers of the form $a + ib$ are unique and at most one of them can be k, there can be no more than one prime in this series. In other words, Dirichlet's theorem asserts that any series $a + ib$ has infinite primes if there is no simple reason to support the contrary. In the previous theorem, we proved a special case of Dirichlet's Theorem for $a = 3$ and $b = 4$.*

Proof: (Sketch) The proof is based on showing that if $gcd(a,b) = 1$, then the series:

$$\sum_{p \equiv_b a} \frac{1}{p}$$

is divergent. If the series is divergent, then indeed there must be infinitely many primes p such that $p \equiv_b a$. Note that $p \equiv_b a$ implies that $p = qb + a$ for some quotient q and $1 \leq a < b$. □

Lemma 8.1 *Let $n \geq 1$ throughout.*

1. $2^n \leq \binom{2n}{n} < 2^{2n}$
2. $\prod_{n<p\leq 2n} p \mid \binom{2n}{n}$
3. *Let $r(p)$ satisfy $p^{r(p)} \leq 2n < p^{r(p)+1}$, then* $\binom{2n}{n} \mid \prod_{p\leq 2n} p^{r(p)}$
4. *If $n > 2$ and $2n/3 < p \leq n$, then $p \nmid \binom{2n}{n}$.*
5. $\prod_{p\leq n} p < 4^n$.

Proof:

1. As $2n - k \geq 2(n-k)$ for $0 \leq k < n$, we have

   $$2^n \leq \frac{2n}{n}\frac{2n-1}{n-1}\cdots\frac{n+1}{1} = \binom{2n}{n}$$

   Also as $\binom{2n}{n}$ is one of the terms in the binomial expansion of $(1+1)^2n$, we have:

   $$\binom{2n}{n} < (1+1)^{2n} = 2^{2n}$$

2. This follows as each prime in the interval $[n+1, 2n]$ divides $(2n)!$ but not $n!$
3. The exponent of p in $n!$ is $\sum_{j=1}^{r(p)}[n/p^j]$. Therefore, the exponent of p in $\binom{2n}{n}$ is

   $$\sum_{j=1}^{r(p)}\{[2n/p^j] - 2[n/p^j]\} \leq \sum_{j=1}^{r(p)} 1 = r(p)$$

   The last inequality holds as each term in curly brackets is either 0 or 1. Taking the product over primes $p \leq 2n$, we get the desired result.
4. If p satisfies $2n/3 < p \leq n$, then p occurs once in the prime factorization of $n!$ and twice in $(2n)!$ (as $3p > 2n$), hence as $p > 2$, $p \nmid \binom{2n}{n}$.
5. This is proved by complete induction. Let $P(n)$ denote the proposition to be proved. Clearly $P(1)$, $P(2)$ and $P(3)$ hold, and if $m > 1$, we have $P(2m)$ as:

   $$\prod_{p\leq 2m} p = \prod_{p\leq 2m-1} p < 4^{2m-1} < 4^{2m}$$

So we may suppose $n = 2m+1$ and $m \geq 2$. Each prime p in the interval $[m+2, 2m+1]$ is a factor of $\binom{2m+1}{m}$, hence, if we assume $P(m+1)$ holds,

$$\prod_{p \leq 2m+1} p \leq \binom{2m+1}{m} \prod_{p \leq m+1} p < \binom{2m+1}{m} 4^{m+1}.$$

But $\binom{2m+1}{m}$ is one of the two central terms in the binomial expansion of $(1+1)^{2m+1}$, and so,

$$\binom{2m+1}{m} < \frac{1}{2}(1+1)^{2m+1} = 4^m$$

Thus $P(m+1)$ implies $P(2m+1)$ and the inductive proof is complete.

□

Theorem 8.11 Bertrand's Postulate: *If $n > 0$ then there is a prime p satisfying $n < p \leq 2n$.*

Proof: In order to prove the theorem, we only consider large n. In particular, we assume that the theorem holds for $n < 750$, as it can be observed by inpsection. We present a proof by contradiction. Assume that there exists some large n such that there is no prime p such that $n < p \leq 2n$. Consider the binomial coefficient $\binom{2n}{n}$. From Lemma 8.1, we have that all prime factors p of $\binom{2n}{n}$ satisfy $p \leq 2n/3$. Let $s(p)$ be the largest power of p which divides $\binom{2n}{n}$, so by lemma 8.1, we have

$$p^{s(p)} \leq 2n$$

If $s(p) > 1$, then $p \leq \sqrt{2n}$. It follows that no more than $[\sqrt{2n}]$ primes occur in $\binom{2n}{n}$ with exponent larger than 1. Therefore, we have

$$\binom{2n}{n} \leq (2n)^{\sqrt{2n}} \prod_{p \leq 2n/3} p.$$

Now $\binom{2n}{n} > \frac{4^n}{2n+1}$ (since $\binom{2n}{n}$ is the largest term in the binomial expansion of $(1+1)^{2n}$ which has $2n+1$ summands). Thus we have

$$\frac{4^n}{2n+1} < (2n)^{\sqrt{2n}} \prod_{p \leq 2n/3} p$$

Since $\prod_{p \leq m} < 4^m$, we have

$$\frac{4^n}{2n+1} < (2n)^{\sqrt{2n}} 4^{2n/3}$$

For reasonably large n, we may assume that $2n+1 < (2n)^2$, so canceling $4^{2n/3}$ we have:

$$4^{n/3} < (2n)^{2+\sqrt{2n}}$$

or, taking logarithms,

$$\frac{n \ln 4}{3} < (2 + \sqrt{2n}) \ln 2n$$

This is clearly false for large n. In fact, for $n = 750$, we have

$$325 = \frac{750 \cdot 1.3}{3} < (2 + \sqrt{1500}) \ln 1500 < 41 \cdot 7.5 < 308$$

Hence, the result holds for $n \geq 750$. As mentioned earlier, the result holds by inspection for $n < 750$. □

Conjectures:

- *The twin prime conjecture:* There are many pairs of primes p, q where $q = p + 2$. For examples:

  $$3, 5; \quad 17, 19; \quad 881, 883; \quad 1997, 1999; \quad 10^9 + 7, 10^9 + 9;$$

  Let $\pi_2(x)$ be the number of prime pairs less than x, so for example

  $$\pi_2(10^3) = 35 \quad \text{and} \quad \pi_2(10^6) = 8164$$

  The twin prime conjecture states that

  $$\pi_2(x) \to \infty \qquad \text{as} \qquad x \to \infty$$

  Using very complicated arguments based on the idea of a sieve Chen showed that there are infinitely many pairs of integers p, $p + 2$ where p is a prime and $p + 2$ has at most two prime factors.

- *The Goldbach conjecture:* Any even positive integer, greater than 2, can be expressed as a sum of two primes. For example:

  $$8 = 3 + 5, \quad 80 = 37 + 43, \quad 800 = 379 + 421, \quad 8000 = 3943 + 4057.$$

Chapter 9

Tchebychev's Theorem

9.1 Primes and their Distribution

The following results have been discussed in the earlier chapter

Theorem 9.1 *There is an infinitude of Primes*

Theorem 9.2 $p_n \leq 2^{2^{n-1}}$

Theorem 9.3 *There is an infinite number of primes of the form* $4n+3$

Theorem 9.4 *There is no Arithmetic Progression with all primes*

Theorem 9.5 *If* $n > 2$ *terms of the AP* $p, p+d, ...$ *are all primes, then* $q|d$ *for all primes* $q < n$

Proof: by contradiction. Assume $q < n$ is a prime s.t. $q \not| n$. We claim that the first q terms of the AP yield distinct remainders $\underline{mod}\ q$.$\vdash$ by contradiction suppose $0 \leq i < j < q(p+id)\ \underline{mod}\ q \Leftrightarrow (p+jd)$ $\underline{mod}\ q$. Hence $(j-i)d\ \underline{mod}\ q = 0$. Therefore $q \mid j-i$ or $q \mid d$ and neither is possible. Therefore we have $R = \{a\ \underline{mod}\ q, (a+d)\ \underline{mod}\ q, \ldots (a+(q-1)d)\ \underline{mod}\ q\} = \{0, \ldots q-i\}$ There is a composite $a+id$ with $q \mid a+id$
$\square$

Theorem 9.6 *There are arbitrarily large gaps between primes, i.e. for every positive integer* k*, there exist* k *consecutive composite members.*

Proof: This can be easily seen as $\forall$ positive integers k we have

$$(k+1)! + 2, \ldots, (k+1)! + k + 1. \tag{9.1}$$

$$j \mid (k+1)! + j, \forall j \in 2, \ldots, k+1 \tag{9.2}$$

$\square$

Definition 9.1 $p^\alpha \mid\mid n$ *means* $p^\alpha \mid n$ *but* $p^{\alpha+1} \not| n$

Theorem 9.7 *If for prime p and $n \geq 1$ $p^\alpha \mid\mid n!$ then*

$$\alpha = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor = \sum_{i=1}^{l} \lfloor \frac{n}{p^i} \rfloor \tag{9.3}$$

where $p^l \leq n < p^{l+1}$

Proof: By Induction on n.Clearly $n = 0$ and $n = 1$ are trivial cases. Say this is true for $n - 1$.Therefore we have

$$\beta = \sum_{i=1}^{\infty} \lfloor \frac{n-1}{p^i} \rfloor \text{ and } p^\beta \mid\mid (n-1)! \tag{9.4}$$

Claim 9.1 $\alpha - \beta = k$

Proof:

$$\alpha - \beta = \sum_{i=1}^{l} \lfloor \frac{n}{p^i} \rfloor - \sum_{i=1}^{l} \lfloor \frac{n-1}{p^i} \rfloor = \sum_{i=1}^{l} \left(\lfloor \frac{n}{p^i} \rfloor - \lfloor \frac{n-1}{p^i} \rfloor \right) \tag{9.5}$$

But we know that

$$\left(\lfloor \frac{n}{p^i} \rfloor - \lfloor \frac{n-1}{p^i} \rfloor \right) = \begin{cases} 1 & if\ p^i \mid n \\ o & otherwise \end{cases} \tag{9.6}$$

And therefore

$$\alpha - \beta = k \tag{9.7}$$

□ We therefore have $\alpha = \beta + k$ where $p^k \mid\mid n$ and hence since $n! = n(n-1)!$ and from above we have $p^\beta \mid\mid (n-1)!$ therefore $p^\alpha \mid\mid n!$ □

Corollary 9.8 *For all m, n prime p for $p^\alpha \mid\mid \frac{n!}{m!}$, $\alpha = \sum_{i\geq 1} \left(\lfloor \frac{n}{p^i} \rfloor - \lfloor \frac{m}{p^i} \rfloor \right)$*

Lemma 9.1 *For any prime p, integer n*

Definition 9.2

$$\mu(p,n) \text{ such that } P^{\mu(p,n)} \mid\mid \binom{2n}{n} \tag{9.8}$$

$$\nu(p,n) \text{ such that } p^{\nu(p,n)} \leq 2n < p^{\nu(p,n)+1} \tag{9.9}$$

then

$$\mu(p,n) \leq \nu(p,n) \tag{9.10}$$

Proof: We know that

$$\binom{2n}{n} = \frac{2n!}{n!n!} \tag{9.11}$$

Now from the previous corollary we get

$$\mu(p,n) = \sum_{i=1}^{\nu(p,n)} \left(\lfloor \frac{2n}{p^i} \rfloor - 2\lfloor \frac{n}{p^i} \rfloor \right) \tag{9.12}$$

for each $j \geq 1$

$$\lfloor \frac{2n}{p^i} \rfloor - 2\lfloor \frac{n}{p^i} \rfloor < \frac{2n}{p^i} - 2\left(\frac{n}{p^i} - 1 \right) = 2 \tag{9.13}$$

but we have

$$\lfloor \frac{2n}{p^i} \rfloor - 2\lfloor \frac{n}{p^i} \rfloor \leq 1 \tag{9.14}$$

therefore we have

$$\mu(p,n) \leq \nu(p,n) \tag{9.15}$$

□

Corollary 9.9

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{\mu(p,n)} \tag{9.16}$$

Lemma 9.2

$$\binom{2n}{n} \mid \prod_{p \leq 2n} p^{\nu(p,n)} \tag{9.17}$$

Proof:

$$p^{\mu(p,n)} \,||\, \binom{2n}{n} \; since \; \mu(p,n) \leq \nu(p,n) \tag{9.18}$$

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{\mu(p,n)} \mid \prod_{p \leq 2n} p^{\nu(p,n)} \tag{9.19}$$

□

Fact 9.10

$$\prod_{n \leq p \leq 2n} p \mid \binom{2n}{n} \tag{9.20}$$

since for every p such that $n \leq p \leq 2n$

$$p \mid (2n)!; p \not| n! \tag{9.21}$$

$$\pi(x) = number\ of\ primes\ \leq x\ for\ all\ positive\ x \in \Re \tag{9.22}$$

Corollary 9.11

$$n^{\pi(2n)-\pi(n)} \leq \binom{2n}{n} \leq (\;2n\;)^{\pi(2n)} \tag{9.23}$$

Proof:

$$\prod_{n<p \leq 2n} p \leq \binom{2n}{n} \leq \prod_{p \leq 2n} p^{\nu(p,n)} \tag{9.24}$$

We know that

$$\prod_{n<p \leq 2n} n \leq \prod_{n<p \leq 2n} p \tag{9.25}$$

and

$$p^{\nu(p,n)} \leq 2n \tag{9.26}$$

$$\prod_{n<p \leq 2n} n \leq \binom{2n}{n} \leq \prod_{p \leq 2n} 2n \tag{9.27}$$

or we have

$$n^{\pi(2n)-\pi(n)} \leq \binom{2n}{n} \leq (\;2n\;)^{\pi(2n)} \tag{9.28}$$

□

Theorem 9.12 *Tchebyshev's Theorem:For $x \geq 2$ and $x \in \Re$*

$$a\frac{x}{logx} < \pi(x) \leq b\frac{x}{logx} \tag{9.29}$$

for some real constants a and b

Proof:

Claim 9.2

$$a = \frac{log2}{4} \tag{9.30}$$

We have

$$\left(\begin{array}{c} 2n \\ n \end{array} \right) \leq \left(\begin{array}{c} 2n \end{array} \right)^{\pi(2n)} \tag{9.31}$$

But since

$$\left(\begin{array}{c} 2n \\ n \end{array} \right) = \prod_{j=1}^{n} \frac{n+j}{j} \geq 2^n \tag{9.32}$$

and since for $j \in \{1, 2, \ldots, n\}$ we have $\frac{n+j}{j} \geq 2$ and since $2^n \leq \left(\begin{array}{c} 2n \end{array} \right)^{\pi(2n)}$ we have taking logarithm on both sides

$$nlog2 \leq \pi(2n)log(2n) \tag{9.33}$$

$$\pi(2n) \geq n\frac{log2}{log(2n)} \tag{9.34}$$

for $x \geq 2$, choose n such that $2n \leq x < 2n+2$. $n \geq 1 \Rightarrow 2n \geq 2 \Rightarrow 4n \geq 2n+2 \Rightarrow n \geq \frac{2n+2}{4}$. Therefore

$$\pi(2n) \geq \frac{2n+2}{4}\frac{log2}{logx} \geq \frac{log2}{4}\frac{x}{logx} \tag{9.35}$$

Therefore

$$a = \frac{log2}{4} \tag{9.36}$$

Claim 9.3

$$b = 32log2 \tag{9.37}$$

We have

$$n^{\pi(2n)-\pi(n)} \leq \left(\begin{array}{c} 2n \\ n \end{array} \right) \leq 2^{2n} \tag{9.38}$$

hence we have $\pi(2n) - \pi(n) \leq 2n\frac{log2}{logn}$ where $n > 1$. Let $2n = 2^r$ for $r \geq 3$. Plugging into the previous equation we get

$$\pi(2^r) - \pi(2^{r-1}) \leq 2^r\frac{log2}{log2^{r-1}} = \frac{2^r}{r-1} \tag{9.39}$$

Taking summation on both sides yields

$$\sum_{r=3}^{2j} \left(\pi(2^r) - \pi(2^{r-1}) \right) \leq \sum_{r=3}^{2j} \frac{2r}{r-1} \tag{9.40}$$

or we have

$$\pi(2^{2j}) - \pi(2^2) \leq \sum_{r=3}^{2j} \left(\frac{2^r}{r-1} \right) \tag{9.41}$$

But we know that $\pi(2^2) = 0$, *therefore the above equation yields*

$$\pi(2^j) \leq \sum_{r=3}^{j} \frac{2^r}{r-1} + \sum_{r=j+1}^{2j} \frac{2^r}{r-1} \leq \sum_{r=2}^{j} 2^r + \sum_{r=j+1}^{2j} \frac{2^r}{j} \tag{9.42}$$

But we know that

$$\sum_{r=j+1}^{2j} \frac{2^r}{j} \leq \frac{2^{2j+1}}{j} \text{ and } \sum_{r=2}^{j} 2^r \leq 2^{j+1} \tag{9.43}$$

Therefore we have

$$\pi(2^j) \leq \frac{2^{2j+1}}{j} + 2^{j+1} \tag{9.44}$$

Now since for $j \geq 2$ *we have* $j < 2^j$ *and hence* $2^{j+1}j < 2^{2j+1}$ *and therefore* $2^{j+1} < \frac{2^{2j+1}}{j}$.*Hence*

$$\pi(2^{2j}) \leq 2\frac{2^{2j+1}}{j} \tag{9.45}$$

Hence for $j \geq 2$ *we have*

$$\frac{\pi(2^{2j})}{2^{2j}} \leq \frac{4}{j} \tag{9.46}$$

Clearly this also holds for $j = 1$. *Therefore for any* $x \in \Re$ *there is a unique* j *such that*

$$2^{2j-2} \leq x \leq 2^{2j} \tag{9.47}$$

and hence

$$\frac{\pi(x)}{x} \leq \frac{\pi(2^{2j})}{2^{2j-2}} = 4\frac{\pi(2^{2j})}{2^{2j}} < \frac{16}{j} \tag{9.48}$$

Also taking logarithms on both sides in the previous equation we have

$$(2j-2)\, log2 \leq logx \leq 2jlog2 \tag{9.49}$$

Therefore

$$\frac{1}{j} \leq 2\frac{log2}{logx} \tag{9.50}$$

And therefore finally we have

$$\frac{\pi(x)}{x} \leq 32\frac{log2}{logx} \tag{9.51}$$

And hence the result.

□

Chapter 10

Linear congruences, Chinese Remainder Theorem and Fermat's Little Theorem

10.1 Linear Diophantine Equations

Definition 10.1 *Diophantine equations are equations with integer coefficients and which admit only integral solutions.*

The simplest Diophantine equation is of the form:

$$ax + by = c \tag{10.1}$$

Such an equation is called a Linear Diophantine Equation(LDE) in 2 unknowns. We now state the necessary and sufficient conditions for such an equation to have an integral solution.

Theorem 10.1 *The LDE $ax + by = c$ has a solution iff $gcd(a, b)|c$.*

Proof:
($\Longrightarrow$) If (x_0, y_0) is a solution, then $gcd(a, b)|(ax_0 + by_0)$. Clearly then $gcd(a, b)$ also divides the RHS, viz. c.
($\Longleftarrow$) Using extended Euclid's algorithm, find (x_0, y_0) such that $ax_0 + by_0 = d$ where $d = gcd(a, b)$. Since $d|c$, $(x_0c/d, y_0c/d)$ is an integral solution of the original LDE. □

Theorem 10.2 *The set of all solutions of the LDE $ax+by = c$ is given by: $x = x_0 - (b/d)u$, $y = y_0 + (a/d)u$, where (x_0, y_0) is a particular solution and $d = gcd(a, b)$.*

Proof: Let $d = gcd(a, b)$, $a = rd$ and $b = sd$.
Let (x_0, y_0) be a particular solution and (x', y') be any other solution of the LDE.

$$ax_0 + by_0 = c = ax' + by' \tag{10.2}$$
$$\Rightarrow \quad a(x_0 - x') = b(y' - y_0) \tag{10.3}$$
$$\Rightarrow \quad r(x_0 - x') = s(y' - y_0) \tag{10.4}$$
$$\Rightarrow \quad r|(y' - y_0) \wedge s|(x_0 - x') \quad \text{because } gcd(r, s) = 1 \tag{10.5}$$

Therefore, $\exists u$, s.t $x' = x_0 - su = x_0 - (b/d)u$ and $y' = y_0 + ru = y_0 + (a/d)u$. □

We now give a procedure that computes a particular solution for the given LDE. All the other solutions can be derived using this particular solution.

Algorithm 10.1 Solving a Linear Diophantine Equation

Procedure$(LDE(ax + by = c))$
    Let $(d, x', y') = ExtendedEuclid(a, b)$.
    If $d|c$ *then*
        $x_0 \leftarrow cx'/d$
        $y_0 \leftarrow cy'/d$
        return (x_0, y_0)
    else print "No solutions"
EndProc.

Note that Algorithm 10.1 is merely a restatement of Theorem 10.1 which gives a constructive guideline for solving any given LDE.

10.2 Linear congruences

Definition 10.2 *Let a, b, n be integers. Then a is said to be congruent to b modulo m, denoted as*

$$a \equiv b \text{ mod } m \text{ or alternatively as } a \equiv_m b \tag{10.6}$$

if $m|(a - b)$.

Properties of linear congruences

1. $a_1 \equiv_m b_1 \ \wedge \ a_2 \equiv_m b_2 \ \Rightarrow \ a_1 \pm a_2 \equiv_m b_1 \pm b_2$
2. $a_1 \equiv_m b_1 \ \wedge \ a_2 \equiv_m b_2 \ \Rightarrow \ a_1 a_2 \equiv_m b_1 b_2$
3. $ac \equiv_m bc \ \Rightarrow \ a \equiv_{m'} b$ where $m' = m/gcd(c, m)$
4. Given a fixed integer m, for each integer a, there is an integer r, such that $0 \leq r < m$ and $a \equiv_m r$.

These properties can be easily proved by expressing $a \equiv_m b$ as $a = b + km$. We prove Property 4 which leads to some interesting results.

Proof: (Property 4) Define $\mathcal{Z}_m = \{0, 1, \ldots, m-1\}$. This is the set of all possible remainders when any integer is divided by m. Hence if a leaves a remainder r when divided by m then $a = r + km$ for some k. Therefore $a \equiv_m r$ and $r \in \mathcal{Z}_m$. □

The set $\mathcal{Z}_m$ has some interesting properties.

1. If $a, b \in \mathcal{Z}_m$, then $\forall \circ \in \{+, -, *\}, \exists c \in \mathcal{Z}_m$ s.t $c \equiv_m a \circ b$
2. By Property 1, it is clear that $\equiv_m$ is an equivalence relation over $\mathcal{Z}_m$ which is preserved under modular addition, subtraction and multiplication.

The next thing that comes to the mind is division. The modular counterpart of division is called a 'multiplicative inverse'.

Definition 10.3 *Given integers a, m, an integer b is the multiplicative inverse of a modulo m if $ab \equiv_m 1$. We say that $a^{-1} = b$.*

Note that a multiplicative inverse need not exist for any arbitrary integer a. For example, 2 doesn't have a multiplicative inverse modulo 4. Theorem 10.3 puts down necessary and sufficient conditions for existence of an inverse.

Theorem 10.3 *Elements of $\mathcal{Z}_m$ which have multiplicative inverses are precisely those that are relatively prime to m.*

Proof: Rewrite the equation $ax \equiv_m 1$ as $ax - my = 1$. By Theorem 10.1, this LDE can be solved iff $gcd(a, m) = 1$. □

Corollary 10.4 *If p is prime, then all elements in $\mathcal{Z}_p$ except 0 have multiplicative inverses.*

Note that by Property 1, it is clear that $\langle \mathcal{Z}_m, +, 0 \rangle$ and $\langle \mathcal{Z}_p - \{0\}, *, 1 \rangle$ (where p is prime) are abelian groups. Further, $\langle \mathcal{Z}_p, +, *, 0, 1 \rangle$ is a commutative ring.

We now come to solving single variable linear congruences and demonstrate the correspondence between the congruences and LDEs.

Theorem 10.5 *$ax \equiv_m b$ has a solution iff $gcd(a, m)|b$. If $d = gcd(a, m)$ and $d|b$ then $ax \equiv_m b$ has d mutually incongruent solutions modulo m.*

Proof: The congruence can be rewritten as a linear Diophantine equation

$$ax - my = b \tag{10.7}$$

The first part of the proof is obvious from Theorem 10.1. Now, if (x_0, y_0) is a particular solution, then from Theorem 10.2, we know that all solutions of this LDE are given by:

$$x'_u = x_0 + (m/d)u, \ y'_u = y_0 + (a/d)u. \tag{10.8}$$

We claim that $(x'_0, y'_0), (x'_1, y'_1), \ldots, (x'_{d-1}, y'_{d-1})$ are mutually incongruent solutions. Take any two distinct solutions, say (x'_i, y'_i) and (x'_j, y'_j) and let $0 \leq i < j < d$. Therefore,

$$x'_j - x'_i = (j - i)m/d \tag{10.9}$$

Clearly, if $m|(x'_j - x'_i)$ then $d|(j - i)$ which is not possible because $1 \leq j - i \leq d - 1$. So (x'_i, y'_i) and (x'_j, y'_j) are incongruent. Since i and j were arbitrary, $\{(x'_u, y'_u)|0 \leq u < d\}$ consists of mutually incongruent solutions. □

Corollary 10.6 *If $gcd(a, m) = 1$ then a has a unique multiplicative inverse modulo m.*

10.3 Chinese Remainder Theorem

Theorem 10.7 [Chinese Remainder Theorem] *Let $m_1, \ldots, m_r$ be pairwise relatively prime numbers. Then the system of equations*

$$x \equiv_{m_i} a_i \quad (1 \leq i \leq r) \tag{10.10}$$

has a unique solution modulo M, where $M = \prod_{i=1}^{r} m_i$.

Proof: Let $M = \prod_{i=1}^{r} m_i$, and $M_i = M/m_i$. Now,

$$i \neq j \Rightarrow gcd(m_i, m_j) = 1 \tag{10.11}$$
$$\Rightarrow \quad gcd(M_i, m_i) = 1 \tag{10.12}$$
$$\Rightarrow \quad M_i^{-1} \text{ (modulo } m_i) \text{ exists and is unique (Theorem 10.5)} \tag{10.13}$$

Define $x_0 = \sum_{i=1}^{r} M_i M_i^{-1} a_i$. Now by definition of M_i, if $i \neq j$ then $m_j | M_i$. Therefore,

$$\forall j, \quad x_0 \equiv_{m_j} M_j M_j^{-1} a_j \equiv_{m_j} a_j \tag{10.14}$$

Hence, x_0 is a solution of the system of equations. We claim that x_0 is unique modulo $M = \prod_{i=1}^{r} m_i$. Let x_0' be another solution of the system. Therefore,

$$\forall i, \quad x_0 \equiv_{m_i} x_0' \tag{10.15}$$
$$\Rightarrow \quad \forall i, \quad m_i | (x_0 - x_0') \tag{10.16}$$

Now since $i \neq j \Leftrightarrow gcd(m_i, m_j) = 1$, so $(m_1 m_2 \ldots m_r) | (x_0 - x_0')$. Therefore,

$$\prod_{i=1}^{r} m_i (= M) | (x_0 - x_0') \tag{10.17}$$

Hence, x_0 is unique modulo $M = \prod_{i=1}^{r} m_i$ □

10.4 Fermat's Little Theorem

Theorem 10.8 [Fermat's Little Theorem] *If p is prime, then for any integer a, $a^p \equiv_p a$.*

Proof: If $p|a$, then $a^p \equiv_p 0 \equiv_p a$. So let us assume that p doesn't divide a. Consider the numbers $a, 2a, 3a, \ldots, (p-1)a$.

Claim: Any two distinct numbers from the above sequence are incongruent modulo p.
Take any two numbers from the sequence, say ia and ja where $i < j$. Then, $ia \equiv_p ja \Rightarrow p|(j-i)$ since p doesn't divide a. But $1 \leq i < j < p$, so p cannot divide $j - i$. Hence ia and ja are incongruent modulo p.
Therefore, for each element ia, $\exists j$, s.t,

$$ia \equiv_p j \tag{10.18}$$

where, $1 \leq j < p$ and j is determined uniquely by i. Multiplying Eq. 10.18 over all i, we get:

$$1.2\ldots(p-1)a^{p-1} \equiv_p \prod_{j \in \{1,2,\ldots,p-1\}} j \tag{10.19}$$
$$(p-1)!a^{p-1} \equiv_p (p-1)! \tag{10.20}$$
$$a^{p-1} \equiv_p 1 \quad \text{Since } gcd((p-1)!, p) = 1 \tag{10.21}$$
$$a^p \equiv_p a \tag{10.22}$$

Note that when we vary i in the LHS of Eq. 10.18, we get a different value of j each time. This accounts for the $(p-1)!$ term in the RHS of subsequent equations. □

Theorem 10.9 *If $a^p \equiv_q a$ and $a^q \equiv_p a$ where $p \neq q$ are primes, then $a^{pq} \equiv_{pq} a$.*

Proof: By Fermat's Little Theorem, we have $a^p \equiv_p a$, Taking exponents on both sides,

$$a^{pq} \equiv_p a^q \equiv_p a \tag{10.23}$$

Similarly,

$$a^{pq} \equiv_q a^p \equiv_q a \tag{10.24}$$

Hence,

$$p|a^{pq} - a \text{ and } q|a^{pq} - a \tag{10.25}$$

Since $gcd(p, q) = 1$, we have

$$pq|a^{pq} - a \tag{10.26}$$

Hence,

$$a^{pq} \equiv_{pq} a \tag{10.27}$$

□

Chapter 11

Euler's ϕ function, Generalisation of FLT, CRT

11.1 Introduction

In this lecture, we will discuss Euler′s Theorem, Generalisation of Fermat Little Theorem and Chinese Remainder Theorem.

11.2 EULER′s PHI-FUNCTION

For $n \geq 1$, The number $\phi(n)$ denote the number of postive integer not exceeding n , that are relatively prime to n.

Example 11.1 $\phi(1) = 1$ $\quad \phi(2) = 1$ $\quad \phi(3) = 2$ $\quad \phi(4) = 2 \ldots$
$\phi(7) = 6$ $\quad \phi(10) = 4$ $\quad \phi(30) = 8$ $\quad \ldots$

Fact 11.1 $\phi(1) = 1$ $\quad$ *since* $gcd(1,1) = 1$
for $n > 1$ $\quad gcd(n,n) = n \neq 1 \Rightarrow$ *n is not relatively prime to n.*

Definition 11.1 *For $n \geq 1$, $\phi(n)$ can be characterised as the number of postive integers less than n and relatively prime to it. The function ϕ is usually called the Euler phi-function after its originator , (sometimes the totient), the functional notion $\phi(n)$, however, is credited to Gauss.*

$$\phi(n) = |\ \Phi(n)\ |$$
$$\text{where} \quad \Phi(n) = \{\ m_i \ \mid 0 < m_i \leq \text{n}\ ,\ \ m_i \text{ are relatively prime to n }\}$$

Fact 11.2 *if n is prime then every number less than n is relatively prime to it , ie* $\phi(n) = n - 1$.

Theorem 11.3 *if p is a prime and* $k > 1$ *, then*

$$\phi(p^k) = p^k - p^{k-1} = p^k(1 - \tfrac{1}{p})$$

Proof gcd (n, p^k) = 1 if and only if p does not divide n.
There p^{k-1} integers between 1 and p^k which are divisible by p , namely p , 2p , 3p , . . . , ($p^k - 1$)p.
Thus the set { 1 , 2 , . . . , p^k } contains exactly $p^k - p^{k-1}$ integers which are relatively prime to p^k so by definition of ϕ, $\phi(p^k) = p^k - p^{k-1}$

Example 11.2 $\phi(9) = \phi(3^2) = 3^2 - 3 = 6$ $\{1, 2, 4, 5, 7, 8\}$
$\phi(16) = \phi(4^2) = 2^4 - 2^3 = 8$ $\{1, 3, 5, 7, 9, 11, 13, 15\}$

Theorem 11.4 *The function ϕ is a multiplicative function*
$$\phi\ (m\ n) = \phi\ (m)\ \phi\ (n)$$
whenever m and n have no common factor (gcd(m , n) = 1)

Theorem 11.5 *If an integer n > 1 has the prime factorisation $n = p_1^{k_1}\ p_2^{k_2}\ \ldots\ p_r^{k_r}$ then*

$$\phi\ (n) = (p_1^{k_1} - p_1^{k_1-1})\ (p_2^{k_2} - p_2^{k_2-1})\ \ldots\ (p_r^{k_r} - p_r^{k_r-1})$$

$$\phi\ (n) = n\ (1 - \tfrac{1}{p_1})\ (1 - \tfrac{1}{p_2})\ \ldots\ (1 - \tfrac{1}{p_r})$$

Proof By Induction on r , the number of distinct prime factors of n . It is true for $r = 1$, Then $\phi(p_1^{k_1}) = (p_1^{k_1} - p_1^{k_1-1})$. Let it holds for $r = i$, since gcd ($p_1^{k_1}\ p_2^{k_2}\ \ldots\ p_i^{k_i}, p_{i+1}^{k_{i+1}}$) = 1. Now, by definition of multiplicative function -

$$\phi((p_1^{k_1}\ p_2^{k_2}\ \ldots\ p_i^{k_i})p_{i+1}^{k_{i+1}}) = \phi(p_1^{k_1}\ \ldots p_i^{k_i})\ \phi(p_{i+1}^{k_{i+1}})$$
$$= \phi(p_1^{k_1}\ \ldots p_i^{k_i})\ (p_{i+1}^{k_{i+1}} - p_{i+1}^{k_{i+1}-1})$$

Invoking the induction assumption first factor on right hand side becomes

$$\phi(p_1^{k_1}\ \ldots\ p_{i+1}^{k_{i+1}}) = (p_1^{k_1} - p_1^{k_1-1})\ \ldots\ (p_i^{k_i} - p_i^{k_i-1})\ (p_{i+1}^{k_{i+1}} - p_{i+1}^{k_{i+1}-1})$$

This serve to complete the induction step, as well as the proof.

Example 11.3 $\phi(360)$
prime factor of 360 = $2^3 3^2 5$
So $\phi\ (360) = 360(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 96$

Theorem 11.6 *for n>2 , $\phi(n)$ is an even integer.*

Proof Consider two cases when n is power of 2 and when n is not power of two .
(1) Let n is a power of 2 $n = 2^k$ $k \geq 2$
ϕ (n) $= \phi(2^k) = 2^k(1 - \frac{1}{2}) = 2^{k-1}$ ie `even integer`
(2) n does not happen to be power of 2 then it divisible by an odd prime p , then n = p^k m where k $\geq$ 1 and gcd(p^k, m) = 1
By multiplicative nature of phi-function -
ϕ (n) = $\phi(p^k$ m) = $\phi(p^k)$ ϕ (m) = $p^{k-1}(p-1)\phi$ (m)
Hence $\phi(n)$ is even because 2 | $p - 1$.

11.3 FERMAT's THEOREM

Theorem 11.7 *Let p denote prime integer. If p does not divide a then* $a^{p-1} \equiv_p 1$
So for every integer a , $a^p \equiv_p a$

Proof Euler in his landmark result generalized this theorem for any integer (described in next section), so proof of this theorem can be obtained as a corollary to next theorem.

11.4 EULER′s GENERALIZATION of FERMAT′s THEOREM

Theorem 11.8 *for any integer n >1 , if gcd(a,n) = 1, then* $a^{\phi(n)} \equiv_n 1$

Example 11.4 $n = 30, \quad a = 11,$
we have $11^{\phi(30)} \equiv_{30} 11^8 \equiv_{30} 121^4 \equiv_{30} 1^4 \equiv_{30} 1$

As a preclude to launching our proof of Euler′s Generalization of Fermet′s theorem , we require a preliminary lemma -
Lemma Let n > 1, gcd(a,n)=1, if m1 , m2 , . . . , $m_{\phi(n)}$ are the postive integers less than n and relatively prime to n , then am1 , am2 , am3 , . . . , $am_{\phi(n)}$ are congruent modulo n to m1 , m2 , . . . , $m_{\phi(n)}$ in some order.

if gcd (a, n) = 1 , and Let $\Phi(n) = \{$ m1 , m2 , . . . , $m_{\phi(n)} \}$ Then $\{am_i \mid m_i \in \Phi(n)\} \equiv_n \Phi(n)$ in some order

Proof
<u>*fact*1</u> Observe that no two of the integers am1 , am2 , am3 , . . . , $am_{\phi(n)}$ are congruent modulo n .
$am_i \not\equiv_n am_j$ for all $i \neq j$
otherwise $m_i \equiv_n m_j$
<u>*fact*2</u> since gcd (a, n) = 1 gcd(m_i, n) = 1 ⇒ gcd (am_i, n) = 1 for all i 1 ≤ i ≤ ϕ(n) , from these two facts $am_i \equiv_n m_j \in \Phi(n)$ for some j.
This proves that the number am1 , am2 , am3 , . . . , $am_{\phi(n)}$ and numbers m1 , m2 , m3 , . . . , $m_{\phi(n)}$ are identical (modulo n) in certain order.

Theorem 11.9 *n*$\in Z^+$ *and gcd (a, n) = 1 , then* $a^{\phi(n)} \equiv_n 1$

Proof Let n>1. Let m1 , m2 , m3 , . . . , $m_{\phi(n)}$ be postive integer less than n which are relatively prime to n. Then m1 , m2 , m3 , . . . , $m_{\phi(n)}$ be reduced residue system modulo n.
⇒ am1 , am2 , am3 , . . . , $am_{\phi(n)}$ is also reduced residue system modulo n.
hence corrosponding to each m_i there is one and only one am_j such that $m_i \equiv_n am_j$ So from previous lemma, am1 , am2 , am3 , . . . , $am_{\phi(n)}$ are congruent, not necessarily in order of appearance, to m1 , m2 , m3 , . . . , $m_{\phi(n)}$ So on taking the product of these $\phi(n)$ congruences, we get -

$$\prod_{i=1}^{\phi(n)} am_i \equiv_n \prod_{i=1}^{\phi(n)} m_i$$
$$\Rightarrow \quad a^{\phi(n)} \prod_{i=1}^{\phi(n)} m_i \equiv_n \prod_{i=1}^{\phi(n)} m_i$$
$$a^{\phi(n)} \equiv_n 1$$

since $gcd(m_i, n) = 1$ and $\prod m_i$ has inverse modulo n , so we cancel out this from both side.
`case` if p is prime, Then $\phi(p) = p - 1$ so, whenever $gcd(a, p) = 1$, we get

$$a^{\phi(p)} \equiv_p 1 \Rightarrow a^{p-1} \equiv_p 1$$

`which is Fermat′ Theorem`

11.5 GAUSS′s THEOREM

Gauss noticed some remarkeble features of phi-function, namely, that sum of the values of $\phi(d)$, as d ranges over the postive divisors of n, is equal to n itself.

For each postive integer n $\geq$ 1 n = $\sum_{d\|n} \phi(d)$ The sum being extended over all postive divisors of n.

Proof The integers between 1 and n can be partitioned into classes such that each class S_d = { m | gcd(m, n) = d , 1≤ m ≤ n } where d | n
ie if d is postive divisor of n, we put the integer m in the class S_d provided gcd(m, n) = d

$$S_1 = \Phi \text{ (n)} \qquad S_n = \{n\}$$

claim : S_d = Φ (n/d) for each d | n, since gcd (m, n) = d ; if and only if gcd (m/d, n/d) = 1
Thus the number of integers in class S_d is equal to number of postive integers not exceeding n/d which are relatively prime to n/d, in other words, equal to ϕ (n/d)
| S_d | = { m | gcd (m/d , n/d) = 1 } = ϕ (n/d)
Then m is in S_d if and only if m/d is in Φ (n/d)
$\sum_{d|n} \phi(d) = \sum_{d|n} \phi(n/d) = \sum_{d|n} |S_d| = n$

Example 11.5 *Let n = 10 , so postive divisors of n are 1 , 2 , 5 , 10 . So the classes S_d are :*

$$S_1 = \{1,\ 3,\ 7,\ 9\} \quad S_2 = \{2,\ 4,\ 6,\ 8\}$$
$$S_5 = \{\ 5\ \} \quad S_{10} = \{\ 10\ \}$$

$$\phi(1) = 1 \quad \phi(2) = 1 \quad \phi(5) = 4 \quad \phi(10) = 4$$

$$\Rightarrow \sum_{d|n} \phi(d) = \sum_{d|n} \phi(n/d) = \sum_{d|n} |S_d| = n$$

Theorem 11.10 *For n>1, the sum of postive integers less than n and relatively prime to n is $\frac{1}{2}n\phi(n)$.*

$$\sum_{gcd(k,n)=1;1\leq k<n} \text{k} = \frac{1}{2}n\phi(n)$$

Proof Let k1, k2, ... $k_{\phi(n)}$ be the postive integers less than n and relatively prime to n. Now,since gcd(k , n) = 1 if and only if gcd(n-k , n) = 1, Then
k1 + k2 + ... + $k_{\phi(n)}$ = (n - k1) + (n - k2) + ... + (n - $k_{\phi(n)}$) = $\phi(n)$ n - (k1 + k2 + ... + $k_{\phi(n)}$)
So $\sum_{k\in\phi(n)} k = \sum_{k\in\phi(n)}(n-k) = \phi(n)n - \sum_{k\in\phi(n)} k$. Thisemplies $\sum_{k\in\phi(n)} k = \frac{1}{2}n\phi(n)$

Example 11.6 *n = 30 ,* $\phi(30) = 8$ *these 8 integers { 1, 7, 11, 13, 17, 19, 23, 29} are less than 30 and are relatively prime to 30 . Then $\sum$ {1, 7, 11, 13, 17, 19, 23, 29} = 120 = $\frac{1}{2}$ 30 8*

11.6 Different Proof of CRT

Euler′s generalisation of Fermat Little Theorem leads to a different proof of Chinese Remainder Theorem. if gcd (m_i, m_j) = 1 for i $\neq$ j . Then system of linear congruences x $\equiv_{m_i} a_i$,for i = 1,2, ..., r

admits a simultaneous solution.
Let M $= \prod_{i=1}^{r} m_i$ $\quad M_i = \frac{M}{m_i}$
The integer $x = a_1 M_1^{\phi(m_1)} + \ldots + a_r M_r^{\phi(m_r)} = \sum_{i=1}^{r} a_i \ M_i^{\phi(m_i)}$ full-fills our requirements. Hence x $\equiv_{m_i}$ $a_i \ M^{\phi(m_i)}$ but since gcd (M_i, m_i) =1 , we have

$$M_i^{\phi(m_i)} \equiv_{m_i} 1$$

and so x $\equiv_{m_i}$ a_i for each i.
This application is one of the usefulness of Euler's Theorem in Number Theory.

11.7 Significance of CRT

$$a \rightleftharpoons (a_1, a_2, \ldots, a_r)$$
$$b \rightleftharpoons (b_1, b_2, \ldots, b_r)$$
these representation are unique upto M = $\prod m_i$
$$(a \pm b) \ \underline{mod} \ M \rightleftharpoons ((a_1 \pm b_1)\underline{mod} m_1, (a_2 \pm b_2)\underline{mod} m_2, \ldots, (a_r \pm b_r)\underline{mod} m_r)$$

(ab) $\underline{mod}$ M
$= (\sum_{i=1}^{r} a_i \ M_i^{\phi(m_i)})(\sum_{j=1}^{r} b_j \ M_j^{\phi(m_j)}) \ \underline{mod}$ M
$= (\sum_{i,j=1}^{r} a_i \ bj \ M_i^{\phi(m_i)} M_j^{\phi(m_j)}) \ \underline{mod}$ M for all i $\neq$ j , M $|$ $M_i^{\phi(m_i)} M_j^{\phi(m_j)}$
$\equiv_M \ \sum_{i=1}^{r} \ a_i b_i M_i^{2\phi(m_i)}$ is a unique solution of system of equation modulo M
$\rightleftharpoons (\ (a_1 b_1) \ \underline{mod} \ m_1, \ \ldots \ , (a_r b_r) \ \underline{mod} \ m_r)$

Chapter 12

Congrunces of Higher Degree

Definition 12.1 *Let a, b, n be integers. Then a is said to be congruent to b modulo m, denoted as*

$$a \equiv b \; mod \; m\$or \; alternatively \; as \; a \equiv_m b \tag{12.1}$$

if $m|(a-b)$.

Definition 12.2 *Let f(x) be any polynomail with integer coefficients then higher order congruence equation will typically look like this.*

$$f(x) \equiv_m 0 \tag{12.2}$$

Fact 12.1 *if all coeffients of the polynomial are multiples of m then every integer is a solution to the equation 2.2.*

Theorem 12.2 *if we primie factorize m then m can be represented as $m = \prod_{i=1}^{k} p_i^{\alpha_i}$ such that $p_i^{\alpha_i}|m$, where $\alpha_i \geq 1$ for each i, and $1 \leq i \leq k$ then $f(x) \equiv_m 0$ is equivalent to f(x) $\equiv_{p_i^{\alpha_i}} 0$ for each p_i.*

this is equivalent to the following claims.

Claim 12.1 *if u is a solution of f(x) $\equiv_m$ 0 then u is a solution of every equation f(x) $\equiv_{p_i^{\alpha_i}}$ 0.*

Claim 12.2 *if f(x) $\equiv_{p_i^{\alpha_i}}$ 0 has no solutions for some i, 1 $\leq$ i $\leq$k then f(x)$\equiv_m$0 has no solutions.*

Claim 12.3 *if each of f(x) $\equiv_{p_i^{\alpha_i}}$ 0 has solutions $a_i^1, a_i^2, \ldots a_i^{k_i}$ which are all mutually incongurent solutions then take u as any linear combination of solutions $u \equiv_m \sum_{i=1}^{k} m_i b_i a_i^{j_i}$ where $m_i = m/p_i^{\alpha_i}$ and $b_i \equiv_{p_i^{\alpha_i}} m_i^{-1}$ and the resulting value u is a solution of f(x) $\equiv_m 0$.*

Proof:
proof for the first claim is
if f(x) $\equiv_m$ 0 has a solution u then

1. f(u) $\equiv_m$ 0 then $m|f(u)$
2. $m|f(u)$ implies that $p_i^{\alpha_i}|f(u)$ for each i

3. for each i if $p_i^{\alpha_i}|f(u)$ implies that f(u) $\equiv_{p_i^{\alpha_i}} 0$

□

Proof for the second claim is very similar to the above and it can be easily proven.

Now we will prove our third claim.
Proof:

1. $p_i^{\alpha_i}|m_j \ \forall j \neq i$ (from the construction of m_j.)
2. $u \equiv_{p_i^{\alpha_i}} m_i b_i a_i \equiv_{p_i^{\alpha_i}} a_i$(from the construction of m_i and b_i.)
3. $f(u) \equiv_{p_i^{\alpha_i}} f(a_i) \equiv_{p_i^{\alpha_i}} 0$ from the fact that a_i is a solution $f(u) \equiv_{p_i^{\alpha_i}} 0$.
4. it means that ∀i $p_i^{\alpha_i}|f(u)$.
5. $\prod_{i=1}^{k} p_i^{\alpha_i}|f(u)$ implies that $m|f(u)$
6. $m|f(u)$ implies that $f(u) \equiv_m 0$

□

With that proof our problem of finding a solution to $f(x) \equiv_m 0$ reduces to a problem of finding a solution to $f(x) \equiv_{p_i^{\alpha_i}} 0$, where p is a prime.

Fact 12.3 *if $f(x) \equiv_{p_i^{\alpha}} 0$ has a solution u then u is a solution of $f(x) \equiv_{p_i^{\beta}} 0$ for all $1 \leq \beta \leq \alpha$.*

Fact 12.4 *$f(x) = \sum_{i=1}^{n} a_i x^i$, where $a_n \neq 0$ then the kth derivative of f is a polynomial with degree $\leq n - k$.*

Fact 12.5 *tailers expansion of $f(x+h)$ is $f(x) + hf'(x) + \frac{h^2}{2!}f''(x) + \cdots + \frac{h^n}{n!}f^n(x)$, as $f^t(x) = 0$ when $t > n$.*

Theorem 12.6 *solving $f(x) \equiv_{p^\alpha} 0$*

Proof: if r is a solution to $f(x) \equiv_{p^\alpha} 0$ then $f(r) \equiv_{p^t} 0$ for $t = 1, 2, \ldots, \alpha$.

consider $\alpha \geq 2$. if there is a solution u_α^i of $f(x) \equiv_{p^\alpha} 0$ then there is solution $u_{\alpha-1}^{j_i}$ of $f(x) \equiv_{p^{\alpha-1}} 0$ such that $u_\alpha^i \equiv_{p^{\alpha-1}} u_{\alpha-1}^{j_i} + vp^{\alpha-1}$ for some integer v. By applying tailers expansion

$$0 \equiv_{p^\alpha} f(u_\alpha^i) \equiv_{p^\alpha} f(u_{\alpha-1}^{j_i} + vp^{\alpha-1}) \equiv_{p^\alpha} f(u_{\alpha-1}^{j_i}) + f'(u_{\alpha-1}^{j_i})vp^{\alpha-1} \tag{12.3}$$

but $f(u_{\alpha-1}^{j_i}) \equiv_{p^{\alpha-1}} 0$. so from equation (2.3) we can write

$$f'(u_{\alpha-1}^{j_i})v \equiv_p \frac{-1}{p^{\alpha-1}} f(u_{\alpha-1}^{j_i}) \tag{12.4}$$

if we know the solutions of $f(x) \equiv_{p^{\alpha-1}} 0$ then from eq 2.4 we can find all the solutions of v and then $u_{\alpha-1}^{j_i} + vp^{\alpha-1}$ will be solutions of $f(x) \equiv_{p^\alpha} 0$

some times it may happen that there are no v corresponding to some $u_{\alpha-1}^{j_i}$. it only means that there are no solutions of $f(x) \equiv_{p^\alpha} 0$ arising from this particular $u_{\alpha-1}^{j_i}$.

In solving $f(x) \equiv_{p^\alpha} 0$ where $\alpha \geq 2$, we start with the solutions $u_1^{(j)}$ of $f(x) \equiv_p 0$. Picking each one of those solutions and find the possible values for v by solving the equation 2.4 and then from $u_{\alpha-1}^{j_i} + vp^{\alpha-1}$ we can find out the solutions for higher order degrees. □

We have now reduced the problem of solving a $f(x) \equiv_m 0$ to congruences with prime moduli. as before we write $f(x) = \sum_{i=0}^{n} a_i x^i \equiv_p 0$

Theorem 12.7 *if the degree n of $f(x) \equiv_p 0$ is greater than or equal to p, then either every integer is a solution of $f(x) \equiv_p 0$ or there is a polynomial g(x) having integral coefficients,with leading coefficient 1,and such that $g(x) \equiv_p 0$ is of degree less than p and the solutions of $g(x) \equiv_p 0$ are precisely those of $f(x) \equiv_p 0$.*

Proof:

If we divide f(x) by $x^p - x$ we obtain f(x) $= q(x)(x^p - x) + r(x)$ where q(x) is a polynomial with integral coefficients and degree less than p.Fermat's theorem shows that $u^p - u \equiv_p 0$, and hence $f(u) \equiv_p r(u)$ for every integer u.

Therefore if r(x) is zero, or every other coefficient in r(x) is divisible by p, then every integer is a solution of $f(x) \equiv_p 0$.

The only other possibility is $r(x) = \sum_{j=0}^{k} b_j x^j$, where $k < p$, with atleast one coefficient not divisible by p. Let b_k be the coefficient with largest subscript k such that $gcd(p, b_k) = 1$.Then $\exists b$, an integer such that $bb_k \equiv_p 1$ and clearly $r(x) \equiv_p 0$ and $br(x) \equiv_p 0$ have the same solutions. □

Chapter 13

Lagrange's Theorem

Hitesh Chaudhary
hitesh@cse.iitd.ernet.in

13.1 Lecture 12

13.1.1 Theorem 12.1

$f(x) = \sum_{i=0}^{n} a_i x^i$, $a_n \ncong_p 0$ if $n < p$ then
either, (1) every integer is a solution of $f(x)$
or, (2) $\exists g(x)$ with integeral coefficients such that
(a)$deg(g) < p$
(b) leading coefficient is 1
such that the roots of $g(x)$ are precisely the roots of $f(x)$

13.1.2 Theorem 12.2 - Lagrange's Theorem

$f(x) \cong_p 0$ has atmost n mutually incongurant solutions, if not, then every integer is solution.
Also, $deg(f) = n < p$
Proof: *By indution*
Base Case: for $n = 0$; $a_0 = a_n \ncong_p 0$ therefore no solution
Induction Step: Assume theorem is true forall $deg < n$

We need to prove for $deg = n$
Proof by contradiction: Suppose $f(x)$ has more than n roots, $u_1, u_2, \cdots, u_n, u_{n+1}$ and lets $g(x) = f(x) - a_n \prod_{i=1}^{n}(x - u_i)$
Here, $deg(g) < n$ since $deg(f) = n$ & highest order term will be cancelled . Also $u_1, u_2, \cdots, u_n$ are roots of $g(x)$
As g satisfies the theorem $\Rightarrow$ either g has atmost n-1 solution or every integer is its solution.
From above we know g has n solutions $\Rightarrow$ g has all integer solutions
$\forall$ integer v, $g(v) \cong_p 0 \cong_p f(v) - a_n \prod_{i=1}^{n}(x - u_i)$
putting $v = u_{n+1}$, $f(u_{n+1}) = 0$, now $a_n \prod_{i=1}^{n}(x - u_i)$ must be $= 0$
as $a_n \ncong_p 0$
$\Rightarrow p \mid (u_{n+1} - u_n)$ for some i

$\Rightarrow\ u_{n+1} \cong_p u_i$ which is contradiction. Hence $f(x)$ has not more than n roots.

We have:

- $f(x)$ has atmost $min(deg(f), p)$ roots if every integer is not a solution
- $\forall a_i,\ p \mid a_i$, for $deg(f) < p$ *iff* all integers are roots of $f(x)$

13.1.3 Theorem 12.3

$f(x) \cong_p 0$ with $a_n \cong_p 1$ has n mutually incongruent solutions *iff*
$x^p - x = f(x)q(x) + p\,s(x)$
(note: $deg(s) < n$ as we are dividing $x^p - x$ by $f(x)$)
Proof: $(\Rightarrow)$
Suppose $f(x)$ has n roots then $x^p - x = f(x)q(x) + r(x)$ where $r(x) = 0$ or $deg(r) < n$
For all solutions u, $f(u) \cong_p 0$, $u \perp p$
$\Rightarrow\ u^p - u \cong_p 0 \cong_p r(u) \Rightarrow\ r(x) = 0\ or\ p \mid r(u)$
This is true for all $u \Rightarrow$ p is factor for every coefficient of $r(x) \Rightarrow r(x) = p\,s(x)$

Proof:$(\Leftarrow)$
Assume, $x^p - x = f(x)q(x) + p\,s(x)$
$\forall$ integers u, By FLT, $u^p - u \cong_p 0$,
also $u^p - u \cong_p 0 = f(u)q(u) + p\,s(u)$. Note, $p\,s(u) \cong_p 0$
$\Rightarrow f(u)q(u) \cong_p 0$
Now, $f(x)q(x)$ is a polynomial of degree p, nth coefficient of $f(x)$, is $\cong_p 1$ and x^p has coefficient 1.
Therefore leading coefficient of $q(x)$ is $\cong_p 1$
Also, $deg(f) = n$ and therefore $deg(q) = p - n$
$f(x)$ and $q(x)$ has atmost n and $p - n$ mutually congruent roots.
(Since leading coefficients of $f(x)$ and $q(x) \cong_p$, therefore all integers are not their roots)
Also $f(x)$ cant have less than n roots otherwise, $deg(f(u)q(u))$ will be less than p
$\Rightarrow\ f(x)$ has exactly n roots.

Theorem(*Cor of Lagranges's Theorem*)

If $d \mid p - 1$ then $x^d - 1 \cong_p 0$ has exactly d solutions
Proof:
By FLT, $(x^d - 1)f(x) = x^{p-1} - 1 \cong_p 0$ where $f(x) = x^d + x^{2d} + \cdots + x^{(k-1)d}$ where $p - 1 = kd$
$\Rightarrow\ x^{p-1} - 1 \cong_p 0 \Rightarrow\ (p-1)$ mutually incongruent solutions
Also, $deg(f) = p - d - 1 \Rightarrow\ f(x)$ has exactly $p - 1 - d$ solutions
Therefore, $x^d - 1$ has exactly d solutions.

Chapter 14

Primitive Roots and Euler's Criterion

14.1 Euler's Criterion and Strengthened Euler's Criterion

The Quadratic Reciprocity Law deals with the solvability of quadratic congruences.It therefore seems appropriate to begin by considering the congruence

$$ax^2 + bx + c \equiv_p 0 \tag{14.1}$$

where p is an odd prime and $a \not\equiv_p 0$ that is, $gcd(a,p) = 1$. The supposition that p is an odd prime implies that $gcd(4a,p) = 1$.(if p is even prime i.e 2, then $gcd(4a,2) = 1$ doesnot hold).Thus, congruence (1.1) is equivalent to

$$4a(ax^2 + bx + c) \equiv_p 0.$$

Using the identity

$$4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac)$$

the last-written congruence may be expressed as

$$(2ax + b)^2 \equiv_p (b^2 - 4ac)$$

Now put $y = 2ax + b$ and $d = b^2 - 4ac$ to get

$$y^2 \equiv_p d \tag{14.2}$$

If $x \equiv_p x_0$ is a solution of (1.1), then $y \equiv_p 2ax_0 + b$ satisfies the congruence (1.2).Conversely, if $y \equiv_p y_0$ is a solution of (1.2), then $2ax \equiv_p y_0 - b$ can be solved to obtain a solution of (1.1).
Thus, the problem of finding a solution to the quadratic congruence (1.1) is equivalent to that of finding a solution to a linear congruence and a quadratic congruence of the form

$$x^2 \equiv_p a \tag{14.3}$$

If $p|a$,then (1.3) has $x \equiv_p 0$ as its only solution.To avoid trivialities, let us assume hereafter that $p \not| a$.
Granting this, whenever $x^2 \equiv_p a$ admits a solution $x = x_0$, then there is also a second solution $x = p - x_0((p-x_0)^2 \equiv_p p^2 - 2px_0 + x_0^2 \equiv_p x_0^2 \equiv_p a$.This second solution is not congruent to the first.For $x_0 \equiv_p p - x_0$ implies that $2x_0 \equiv_p 0$,or $x_0 \equiv_p 0$, which is impossible because $p \not| a$.By Lagrange's Theorem, these two solutions

exhaust the incongruent solutions of $x_2 \equiv_p a$. In short: $x_2 \equiv_p a$ has exactly two solutions or no solutions.
The major effort in this presentation is directed towards providing a test for the existence of solutions of the congruence

$$x_2 \equiv_p a, gcd(a, p) = 1$$

To put it differently,we wish to identify those integers a which are perfect squares modulo p.

Definition 14.1 *Let p be an odd prime and gcd(a,p)=1.If the congruence $x^2 \equiv_p a$ has a solution, then a is said to be a* ***quadratic residue*** *of p.Otherwise,a is called a* ***quadratic nonresidue*** *of p.*

The point to be borne in mind is that if $a \equiv b \ mod \ p$, then a is quadratic residue of p, if and only if b is a quadratic residue of p.
Thus,we need only determine the quadratic character of those positive integers less than p in order to ascertain that of any integer.

Theorem 14.1 (Euler's Criterion).Let p be an odd prime and gcd(a,p)=1.Then a is a quadratic residue of p if and only if $a^{\frac{(p-1)}{2}} \equiv_p 1$

Proof: Suppose that a is a quadratic residue of p, so that $x^2 \equiv_p a$ admits solution, call it x_1.Since gcd(a, p)=1,evidently gcd(x_1, p)=1.We may therefore appeal to Fermat's Theorem to obtain

$$a^{\frac{(p-1)}{2}} \equiv_p (x_1^2)^{\frac{(p-1)}{2}} \equiv_p x_1^{p-1} \equiv_p 1$$

For the opposite direction, assume that $a^{\frac{(p-1)}{2}} \equiv_p 1$ holds and let r be the primitive root of p(The primitive roots are explained in the next section and the proof in the reverse direction can be read after reading next section).Then $a \equiv_p r^k$ for some integer k, with $1 \leq k \leq p-1.a^{(p-1)/2)} \equiv_p r^{k(p-1)/2} \equiv_p 1$
By Theorem 1.3, the order of r (namely,$p-1$) must divide the exponent $k(p-1)/2$.The implication is that k is an even integer, say $k = 2j$.Hence

$$(r^j)^2 = r^{2j} = r^k \equiv_p a,$$

making the integer r^j a solution of the congruence $x^2 \equiv_p a$.This proves that a is a quadratic residue of prime p.
Now if p(as always) is an odd prime and gcd(a, p)=1 then

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) = a^{p-1} - 1 \equiv_p 0,$$

the last congruence being justified by Fermat's Theorem.Hence either

$$a^{(p-1)/2} \equiv_p 1 \text{ or } a^{(p-1)/2} \equiv_p -1,$$

but no both.For, if both congruences held simultaneously, then we would have $1 \equiv_p -1$, or equivalently, $2 \equiv_p 0$ implies$p|2$, which conflicts with our hypothesis.Since a quadratic nonresidue of p does not satisfy $a^{(p-1)/2} \equiv_p 1$, it must therefore satisfy ($a^{(p-1)/2} \equiv_p -1$).This observation provides an alternate nonresidue of p if and only if $a^{(p-1)/2} \equiv_p -1$

□

Corollary 14.2 (Strengthened Euler's Criterion). Let p be an odd prime and gcd(a,p)=1.Then a is a quadratic residue or nonresidue of p according as

$$a^{(p-1)/2} \equiv_p 1 \textbf{ or } a^{(p-1)/2} \equiv_p -1$$

14.2 The Order of an Integer Modulo n

Definition 14.2 *Let $n > 1$ and gcd(a,n)=1.The order of a modulo n is the smallest positive integer k such that $a^k \equiv_n 1$*

Observe that if two integers are congruent modulo n, then they have the same order modulo n.For if $a \equiv_n b$, implies that $a^k \equiv_n b^k$, when $b^k \equiv_n 1$.
It should be emphasized that our definition of order n concerns only integers a for which $gcd(a,n) = 1$.Indeed,if $gcd(a,n) > 1$, then we know that the linear congruence $ax \equiv_n 1$ has no solution(The linear congruence $ax \equiv_n b$ has a solution if and only if $d|b$,where $d = gcd(a,n)$.Here $d > 1$ and $b = 1$, so $d \not| b$.) ;hence the relation

$$a^k \equiv_n 1, k \geq 1$$

cannot hold, for this would imply that $x = a^{k-1}$ is a solution of $ax \equiv_n 1$.Thus,whenever there is reference to the order of a modulo n, it is assumed that $gcd(a,n) = 1$,even if it is not explicitly stated.

Theorem 14.3 *Let the integer a have order k modulo n.Then $a^b \equiv_n 1$ if and only if $k|b$; in particular, $k|\phi(n)$.*

Proof: Suppose to begin with that $k|b$, so that $b = jk$ for some integer j.Since $a^k \equiv_n 1$, $(a^k)^j \equiv_n 1^j (a \equiv_n b$ implies $a^k \equiv_n b^k)$ or $a^b \equiv_n 1$.
Conversely, let b be any positive integer satisfying $a^b \equiv_n 1$.By the division algorithm, there exists q and r such that $b = qk + r$, where $0 \leq r < k$,consequently,

$$a^b = a^{qk+r} = (a^k)^q a^r$$

By hypothesis both $a^b \equiv_n 1$ and $a^k \equiv_n 1$, the implication of which is that $a^r \equiv_n 1$.Since $0 \leq r < k$, we end up with $r = 0$;otherwise, the choice of k as the smallest positive integer such that $a^k \equiv_n 1$ is contradicted. Hence $b = qk$ and $k|b$.
Theorem 1.3 expedites the computation when attempting to find the order of an integer a modulo n:instead of considering all powers of a, the exponents can be restricted to the divisors of $\phi(n)$. □

Theorem 14.4 *If a has order k modulo n, then $a^i \equiv_n a^j$ if and only if $i \equiv_k j$.*

Proof: First,suppose that $a^i \equiv_n a^j$,where $i \leq j$.Since a is relatively prime to n, we can cancel a power of a to obtain $a^{i-j} \equiv_n 1$.According to theorem 1.3, this last congruence holds only if $k|i-j$, which is just another way of saying that $i \equiv_k j$.
Conversely, let $i \equiv_k j$.Then we have $i = j + qk$ for some integer q.By the definition of k, $a^k \equiv_n 1$, so that

$$a^j \equiv_n a^{j+qk} \equiv_n a^j (a^k)^q \equiv_n a^j$$

which is the desired conclusion □

Corollary 14.5 *If a has order k modulo n , then the integers $a, a^2, a^3, ..., a^k$ are incongruent modulo n*

Proof: If $a^i \equiv_n a^j$ for $1 \leq i \leq j \leq k$, then the theorem insures that $i \equiv_k j$.But this is impossible unless $i = j$.Hence $a, a^2, .., a^k$ are incongruent modulo n. □

Theorem 14.6 *If the integer a has order k modulo n and $b > 0$, then a^b has order $k|gcd(b,k)$ modulo n.*

Proof: Let $d = gcd(b,k)$.Then we may write $b = b_1 d$ and $k = k_1 d$, with $gcd(b_1, k_1) = 1$.Clearly,

$$(a^b)^{k_1} = (a^{b_1 d})^{k/d} = (a^k)^{b_1} \equiv_n 1$$

If a^b is assumed to have order r modulo n,then theorem 1.3 asserts that $r|k_1$.On the other hand, since a has order k modulo n, the congruence

$$a^{br} \equiv_n (a^b)^r \equiv_n 1.$$

indicates that $k|br$;in other words, $k_1 d|b_1 dr$.But $gcd(k_1, b_1) = 1$ and therefore $k_1|r$.This divisibility relation,when combined with the one obtained obtained earlier($r|k_1$),gives

$$r = k_1 = k/d = k/gcd(b,k)$$

proving the theorem. □

Corollary 14.7 *Let a have oder k modulo n.Then a^b has order k if and only if $gcd(b,k) = 1$.*

14.3 Primitive Roots of Primes

Definition 14.3 *If $gcd(a,n) = 1$ and a is of order $\phi(n)$ modulo n, then a is a* ***Primitive Root*** *of n.*

More generally, one can prove that primitive roots exist for any prime modulus, a result of fundamental importance. While it is possible for a primitive root of n to exist when n is not a prime, there is no reason to expect that every integer n will possess a primitive root;indeed, the existence of primitive roots is more an expection than a rule

Theorem 14.8 *Let $gcd(a,n) = 1$ and let $a_1, a_2, a_3, ..., a_{\phi(n)}$ be the positive integers less than n and relatively prime to n.If a is a primitive root of n,then*

$$a^1, a^2, a^3, ..., a^{\phi(n)}$$

are congruent modulo n to $a_1, a_2, a_3, ..., a_{\phi(n)}$, in some order.

Proof: Since a is relatively prime to n, the same holds for all the powers of a;hence, each a^k is congruent modulo n to some one of the a_i.The $\phi(n)$ numbers in the set $[a^1, a^2, a^3, ..., a^{\phi(n)}]$ are incongruent by the corollary to theorem 1.4.As the powers are incongruent to each other and each one is congruent to some one of a_i,these powers must represent the integers $a_1, a_2, a_3, ..., a_{\phi(n)}$. □ One consequence of what has just been proved is that, in those cases in which a primitive root exists, we can know state exactly how many there are,

Corollary 14.9 *If n has a primitive root, then it has exactly $\phi(\phi(n))$ of them*

Proof: Suppose that a is a primitive root of n.By the theorem, any other primitive root of n is found among the members of the set $[a^1, a^2, a^3, ..., a^{\phi(n)}]$.But the number of powers $a^k, 1 \leq k \leq \phi(n)$, which has order $\phi(n)$ is equal to the number of integers k for which $gcd(k, \phi(n) = 1$(rest of the integers have order less than $\phi(n)$ because for all such integers l, $gcd(l, \phi(n)) > 1$) i.e the power of the a should be relatively prime to $\phi(n)$ for it to be a primitive root.;there are $\phi(\phi(n))$ such integers, hence $\phi(\phi(n))$ primitive roots of n. □

Theorem 14.10 *If p is a prime number and $d|p-1$,then there are $\phi(d)$ incongruent integers having order d modulo p*

Proof: Let $d|p-1$ and $\psi(d)$ denote the number of integers $k, 1 \leq k \leq p-1$, which have order d modulo p.Since each integer between 1 and $p-1$ has order d for some $d|p-1$ (using theorem 1.3),

$$p - 1 = \textstyle\sum_{d|p-1} \psi(d)$$

At the same time,Gauss' theorem tells us that

$$p - 1 = \textstyle\sum_{d|p-1} \phi(d)$$

and so,putting together,

$$\sum_{d|p-1} \psi(d) = \sum_{d|p-1} \phi(d) \tag{14.4}$$

Our aim is to provide that $\psi(d) \leq \phi(d)$ for each divisor d of $p-1$, since this, in conjunction with equation (1.4), would produce the equality $\psi(d) = \phi(d) \neq 0$(otherwise, the first sum would be strictly smaller than the second)

Given an arbitrary divisor d of $p-1$, there are two possibilities:either $\psi(d) = 0$ or $\psi(d) > 0$.If $\psi(d) = 0$, then certainly $\psi(d) \leq \phi(d)$.Suppose that $\psi(d) > 0$, so that there exists an integer a of order d.Then the d integers $a, a^2, ..., a^d$ are incongruent modulo p(if $a^i \equiv_p a^j$ for $1 \leq i < j \leq d$, then $a^{(j-i)} \equiv_p 1$ where $j - i < d$ and hence contradicting that d is the order) and each of them satisfies the polynomial congruence

$$x^d - 1 \equiv_p 0 \tag{14.5}$$

for,$(a^k)^d \equiv_p (a^d)^k \equiv_p 1$.By the corollary to Lagrange's theorem, there can be no other solutions of (1.5).If follows that any integer which has order d modulo p must be congruent to one of $a, a^2, ..., a^d$.But only $\phi(d)$ of the just mentioned powers have order d,namely those a^k for which the exponent k has the property gcd(k, d)=1.Hence, in the present situation,$\psi(d) = \phi(d)$,and the number of integers having order d modulo p is equal to $\phi(d)$.This establishes the result we set out to prove.
□ Taking $d = p - 1$ in the above Theorem, we arrive at

Corollary 14.11 *If p is a prime,then there are exactly $\phi(p-1)$ incongruent primitive roots of p.*

An illustration is afforded by the prime $p = 13$.For this modulus,1 has order 1;12 has order 2;3 and 9 have order 3;5 and 8 have order 4;4 and 10 have order 6; and four integers, namely 2,6,7,11 have order 12.Thus

$$\textstyle\sum_{d/12} \psi(d) = \psi(1) + \psi(2) + \psi(3) + \psi(4) + \psi(6) + \psi(12)$$

$$= 1 + 1 + 2 + 2 + 2 + 4 = 12$$

as it should.Notice too that

$$\psi(1) = 1 = \phi(1),\ \psi(4) = 2 = \phi(4)$$

$$\psi(2) = 1 = \phi(2),\ \psi(6) = 2 = \phi(6)$$

$$\psi(3) = 2 = \phi(3),\ \psi(12) = 4 = \phi(12,)$$

Chapter 15

Quadratic Reciprocity

15.1 Legendre Symbol

Legendre Symbol: for given Prime p and any a

$$\left[\begin{array}{c} a \\ p \end{array}\right] \equiv_p a^{(p-1)/2} \equiv_p \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \\ 0 & \text{if } p|a \\ \text{-1} & \text{if } a \text{ is quadratic non residue of } p \end{cases}$$

Some facts:

1. $\left[\begin{array}{c} a \\ p \end{array}\right] \left[\begin{array}{c} b \\ p \end{array}\right] = \left[\begin{array}{c} ab \\ p \end{array}\right]$
2. $\left[\begin{array}{c} a^2 \\ p \end{array}\right]$=1 given any $\left[\begin{array}{c} a \\ p \end{array}\right]$
3. a $\equiv_p$ b implies $\left[\begin{array}{c} a \\ p \end{array}\right] = \left[\begin{array}{c} b \\ p \end{array}\right]$
4. $\left[\begin{array}{c} 1 \\ p \end{array}\right]$=1
5. $\left[\begin{array}{c} -1 \\ p \end{array}\right] = \begin{cases} 1 & \text{if } p \equiv_4 1 \cdots (i) \\ \text{-1} & \text{if } p \equiv_4 -1 \end{cases}$
   since $p = 4k+1$ or $4k+3$ all primes of the form $(p-1)/2 = 2k$ or $2k+1$
6. $x^2 \equiv_p -1$ has a solution iff p is of the form $4k+1$ (from fact (i))

Theorem 15.1 *For odd prime p,* $\sum_{a=1}^{p} \left[\begin{array}{c} a \\ p \end{array}\right]$*=0*

Proof: if $p|a$ then $\left[\begin{array}{c} a \\ p \end{array}\right]$=0;
else $gcd(a,p) = 1$, so there will be exactly (p-1)/2 a's are quadratic residues of p and remaining (p-1)/2 will be quadratic non residue of p
□

Corollary 15.2 *The quadratic residues of (prime) p are congruent modulo p to the even powers of primitive roots. Conversely, the quadratic non-residues are congruent to odd powers of primitive root.*

15.2 Gauss' Lemma

Theorem 15.3 *For any odd prime p and a such that $a \perp p$*
$S = \{a, 2a, 3a, \ldots (p-1)a/2\}$
$T = \{b \in \mathbf{S} \mid b \ mod \ p \ > \ p \ div \ 2\}$
then $\left\lfloor \begin{array}{c} a \\ p \end{array} \right\rfloor = (-1)^{|T|}$

Proof: The elements of S are all distinct modulo p
We would break set S into two sets $\{r_1, r_2, \ldots r_m\} = U = \{r \mid 0 < r \leq p/2, b \ modp = r, b \ \in \mathbf{S}\}$
and $\{s_1, s_2, \ldots s_n\} = V = \{s \mid p/2 < s < p, b \ modp \ \leq s, b \ \in \mathbf{S}\}$
p being odd prime, $p/2$ is not an integer.
$S = \{r_1, r_2, \ldots r_m\} \cup \{s_1, s_2, \ldots s_n\}$
$m + n = (p-1)/2$

Claim 15.1 $r_1, r_2, \ldots r_m, p - s_1, p - s_2, \ldots p - s_n$ *are all disjoint*

Proof: This follows from the fact that all elements of S are disjoint.
$r_1, r_2, \ldots r_m$ are disjoint
$s_1, s_2, \ldots s_n$ are disjoint
if $r_i = p - s_j$
$\Longrightarrow r_i + s_j = p$
assume r_i came from ka and s_j came from ma then $r_i + s_j \equiv_p 0$
$\Longrightarrow p|(k+m)$
therefore disjoint (both k, m are less than $p/2$ hence $k + m < p$) □
Therefore $\{r_1, r_2 \ldots r_m, p - s_1, p - s_2 \ldots p - s_n\} = \{1, 2, \ldots (p-1)/2\}$
$\prod\{r_1, r_2 \ldots r_m, p - s_1, p - s_2 \ldots p - s_n\} = \prod\{1, 2, \ldots (p-1)/2\} = ((p-1)/2)!$
$((p-1)/2)! = r_1 r_2 \ldots r_m (p - s_1)(p - s_2) \ldots (p - s_n) \equiv_p (-1)^n r_1, r_2, \ldots r_m, s_1, s_2 \ldots s_n$ we know that $\{r_1, r_2 \ldots r_n, s_1, s_2 \ldots s_n\} \equiv_p$ [illegible]
S Therefore $((p-1)/2)! \equiv_p (-1)^n \prod S = (-1)^n a^{(p-1)/2}((p-1)/2)!$
as p is relatively prime to $(p-1)/2$
so we can cancel $((p-1)/2)!$ on both sides
Therefore $a^{(p-1)/2}(-1)^n \equiv_p 1$
multiply both sides with $(-1)^n$
Therefore $a^{(p-1)/2} \equiv_p (-1)^n$
$n = |T|$
$\left\lfloor \begin{array}{c} a \\ p \end{array} \right\rfloor = a^{(p-1)/2} \equiv_p (-1)^{|T|}$
□
Consequence $\left\lfloor \begin{array}{c} 2 \\ p \end{array} \right\rfloor = \begin{cases} 1 & \text{if } p \equiv_8 1 \text{ or } p \equiv_8 7 \\ \text{-1} & \text{if } p \equiv_8 3 \text{ or } p \equiv_8 5 \end{cases}$

$\left\lfloor \begin{array}{c} 2 \\ p \end{array} \right\rfloor = (-1)^n$ where n is the number of numbers in $\{2, 4, 6 \ldots (p-1)\}$ whose remainder $> (p-1)/2$
$S = \{2a \mid 1 <= a <= (p-1)/2\}$
$T = \{b \in \mathbf{S} \mid b > (p-1)/2\}$
$2a \leq (p-1)/2 \ iff \ a <= p \ div \ 4$
$p = 8k + 1 \Rightarrow p \ div \ 4 \ = 2k \ and \ (p-1)/2 = 4k \ \Rightarrow n = 2k$
$p = 8k + 3 \Rightarrow n = 2k + 1$
$p = 8k + 5 \Rightarrow n = 2k + 1$
$p = 8k + 7 \Rightarrow n = 2k + 2$
when $p \equiv_8 1$ or $p \equiv_8 7$ then n is even
Therefore $\left\lfloor \begin{array}{c} 2 \\ p \end{array} \right\rfloor$=1

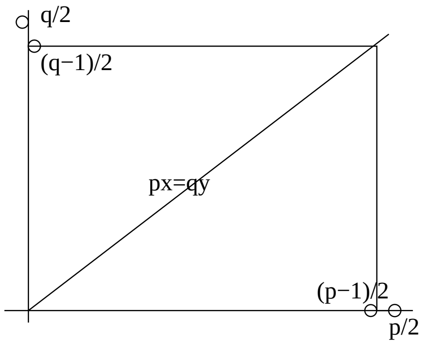


Figure 15.1: Graph

15.3 Gauss' Reciprocity Law

For Odd primes p and q
$\left[\begin{array}{c} p \\ q \end{array}\right]\left[\begin{array}{c} q \\ p \end{array}\right] = (-1)^{((p-1)/2)((q-1)/2)}$

Consider the Lattice points in the rectangle (x, y) where both x, $y \in \mathbf{W}$(Whole Number Set)
Therefore $(p-1)/2)((q-1)/2)$ lattice points in the interior of rectangle.

Claim 15.2 *No Lattice points on the diagonal*

Proof: If there were then $py = qx$
as p & q are distinct and x & y are bounded by $p/2$ & $q/2$ which can't happen
Which means diagonal splits it into two equal triangles.
□

Claim 15.3 $\sum_{j=1}^{(p-1)/2} jq \ div \ p$ *Lattice points in the lower triangle*

Proof: Take any vertical line on integer i.e line $x = j$ where j is an integer.
Then that line has $jq \ div \ p$ lattice points on that line So total number of lattice points in the lower triangle are $\sum_{j=1}^{(p-1)/2} jq \ div \ p$
□

Claim 15.4 $\sum_{i=1}^{(q-1)/2} ip \ div \ q$ *lattice points in the upper triangle*

proof similar to earlier claim

We know already $((p-1)/2)((q-1)/2)$ lattice points
Therefore $((p-1)/2)((q-1)/2) = \sum_{j=1}^{(p-1)/2} jq \ div \ p \ + \sum_{i=1}^{(q-1)/2} ip \ div \ q$
$\left[\begin{array}{c} p \\ q \end{array}\right] = (-1)^m$ where $m = \sum_{j=1}^{(p-1)/2} jq \ div \ p$ (by Gauss' lemma)

$\left\lfloor \begin{matrix} q \\ p \end{matrix} \right\rfloor = (-1)^n$ where $n = \sum_{i=1}^{(q-1)/2} ip\ div\ q$

$\left\lfloor \begin{matrix} p \\ q \end{matrix} \right\rfloor \left\lfloor \begin{matrix} q \\ p \end{matrix} \right\rfloor = (-1)^{((p-1)/2)((q-1)/2)}$ Those lattice points repressent $\{r \mid r = b\ mod\ p\ , b \in \mathbf{S}, 0 < r < p/2\} \& \{s \mid s = b\ mod\ p\ , b \in \mathbf{S}, p/2 < s < p\}$
as equation of diagonal is $py = qx$ Everything above diagonal represents $y > qx/p$ & below diagonal $y < qx/p$

Example 15.1 $\left\lfloor \begin{matrix} 29 \\ 53 \end{matrix} \right\rfloor = \left\lfloor \begin{matrix} 53 \\ 29 \end{matrix} \right\rfloor$ *as* $29 \equiv_4 1$ *and* $53 \equiv_4 1$

$\left\lfloor \begin{matrix} 29 \\ 53 \end{matrix} \right\rfloor = \left\lfloor \begin{matrix} 53 \\ 29 \end{matrix} \right\rfloor = \left\lfloor \begin{matrix} 53\ mod\ 29 \\ 29 \end{matrix} \right\rfloor = \left\lfloor \begin{matrix} 24 \\ 29 \end{matrix} \right\rfloor = \left\lfloor \begin{matrix} 8 \\ 29 \end{matrix} \right\rfloor \left\lfloor \begin{matrix} 3 \\ 29 \end{matrix} \right\rfloor = \left\lfloor \begin{matrix} 2 \\ 29 \end{matrix} \right\rfloor \left\lfloor \begin{matrix} 2 \\ 29 \end{matrix} \right\rfloor \left\lfloor \begin{matrix} 2 \\ 29 \end{matrix} \right\rfloor \left\lfloor \begin{matrix} 3 \\ 29 \end{matrix} \right\rfloor$
as any square gives 1

$= \left\lfloor \begin{matrix} 2 \\ 29 \end{matrix} \right\rfloor \left\lfloor \begin{matrix} 3 \\ 29 \end{matrix} \right\rfloor = (-1) \left\lfloor \begin{matrix} 3 \\ 29 \end{matrix} \right\rfloor$ *(as* $29 \equiv_8 5$*)*

$\left\lfloor \begin{matrix} 3 \\ 29 \end{matrix} \right\rfloor = \left\lfloor \begin{matrix} 29 \\ 3 \end{matrix} \right\rfloor$ *as* $29 \equiv_2 1$ *&* $3 \equiv_2 1$

$\left\lfloor \begin{matrix} 29 \\ 3 \end{matrix} \right\rfloor = \left\lfloor \begin{matrix} 29 mod 3 \\ 3 \end{matrix} \right\rfloor = \left\lfloor \begin{matrix} 2 \\ 3 \end{matrix} \right\rfloor = -1$

Therefore $\left\lfloor \begin{matrix} 29 \\ 53 \end{matrix} \right\rfloor = (-1)(-1) = 1$
Therefore 29 is a perfect square modulo 53.

Chapter 16

Applications of Quadratic Reciprocity

Vipul Jain
vipul@cse.iitd.ernet.in

Theorem 16.1 *Let p be an odd prime and $a = \pm 2^{k_0} p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$ where $p_1, p_2, \ldots, p_m$ are odd primes. Then,*

- $\left\lfloor \begin{matrix} a \\ p \end{matrix} \right\rfloor = \left\lfloor \begin{matrix} \pm 1 \\ p \end{matrix} \right\rfloor \left\lfloor \begin{matrix} p_1 \\ p \end{matrix} \right\rfloor^{k_1} \left\lfloor \begin{matrix} p_2 \\ p \end{matrix} \right\rfloor^{k_2} \cdots \left\lfloor \begin{matrix} p_m \\ p \end{matrix} \right\rfloor^{k_m}$
- $\left\lfloor \begin{matrix} 1 \\ p \end{matrix} \right\rfloor = 1 \ \forall p$
- $\left\lfloor \begin{matrix} -1 \\ p \end{matrix} \right\rfloor = \begin{cases} 1 & \text{if } p \equiv_4 1 \\ -1 & \text{if } p \not\equiv_4 1 \end{cases}$
- $\left\lfloor \begin{matrix} 2 \\ p \end{matrix} \right\rfloor = \begin{cases} 1 & \text{if } p \equiv_8 1 \text{ or } p \equiv_8 7 \\ -1 & \text{if } p \equiv_8 3 \text{ or } p \equiv_8 5 \end{cases}$
- *if $p_i > p$ then,* $\left\lfloor \begin{matrix} p_i \\ p \end{matrix} \right\rfloor = \left\lfloor \begin{matrix} p_i \pmod p \\ p \end{matrix} \right\rfloor$. *So it's sufficient to consider primes $< p$.*

  Proof: *If $a \equiv_p b$, then the congruences $x^2 \equiv_p a$ and $x^2 \equiv_p b$ have exactly the same solutions, if any at all. Thus either both $x^2 \equiv_p a$ and $x^2 \equiv_p b$ are solvable, or none of them has a solution. Hence* $\left\lfloor \begin{matrix} p_i \\ p \end{matrix} \right\rfloor = \left\lfloor \begin{matrix} p_i \pmod p \\ p \end{matrix} \right\rfloor$ *as both p_i and $p_i \pmod p$ are equal modulo p.* □

- *if $p_i < p$*

$$\left\lfloor \begin{matrix} p_i \\ p \end{matrix} \right\rfloor = \begin{cases} \left\lfloor \begin{matrix} p \\ p_i \end{matrix} \right\rfloor & \text{if } p \equiv_4 1 \text{ or } p_i \equiv_4 1 \\ -\left\lfloor \begin{matrix} p \\ p_i \end{matrix} \right\rfloor & \text{if } p \equiv_4 p_i \equiv_4 3 \end{cases}$$

  Proof: $\left\lfloor \begin{matrix} p \\ q \end{matrix} \right\rfloor \left\lfloor \begin{matrix} q \\ p \end{matrix} \right\rfloor = (-1)^{((p-1)/2)((q-1)/2)}$ *from Gauss's reciprocity law. Now, the number ((p-1)/2).((q-1)/2) is even if and only if at least one of the integers p and q is of the form 4k + 1. If both are of the form 4k + 3, then ((p-1)/2).((q-1)/2) is odd.* □

Claim 16.1 *$2x_0y \equiv_p -b$ has a unique solution.*
Proof: Given equation has a solution if $gcd(2x_0, p)| - b$.
For unique solution, $gcd(2x_0, p)$ = 1.
$gcd(2x_0, p) = gcd(x_0, p)$ as p is odd prime. If $gcd(x_0, p) > 1$, it can only be p as p is prime.
Let $gcd(x_0, p) = p$.
$gcd(x_0, p) = p \Rightarrow p|x_0 \Rightarrow x_0 = c.p$
$\Rightarrow x_0^2 = c^2.p^2 = b.p^n + a \Rightarrow a = 0asa \perp p$.
But a is not zero. Hence we get a contradiction if $gcd(x_0, p) = p$.
Hence $gcd(x_0, p) = 1 \Rightarrow 2x_0 \perp p$
Hence $2x_0y \equiv_p -b$ has a unique solution. □

Theorem 16.2 *If p is an odd prime with $a \perp p$, then $x^2 \equiv_{p^n} a$ has a solution iff $\left\lfloor \begin{matrix} a \\ p \end{matrix} \right\rfloor = 1$.*

Proof: ($\Rightarrow$) Let u be a solution of $x^2 \equiv_{p^n} a$.
$u = x^2 = q.p^n + a \equiv_p a$
$\therefore$ a is a quadratic residue of p and hence $\left\lfloor \begin{matrix} a \\ p \end{matrix} \right\rfloor = 1$

($\Leftarrow$) Let $\left\lfloor \begin{matrix} a \\ p \end{matrix} \right\rfloor = 1$ $(\Rightarrow) x^2 \equiv_p a$ has a solution u. Proof is by induction on n.
Induction Hypothesis: Assume $x^2 \equiv_{p^n} a$ has a solution x_0.
To prove: $x^2 \equiv_{p_{n+1}}$ has a solution $x_0^2 = b.p^{n+1} + a$
From previous claim, let $2x_0y \equiv_p -b$ has unique solution y_0.
Then, $2x_0y_0 \equiv_p -b \Rightarrow p|2x_0y_0 + b \Rightarrow 2x_0y_0 + b = dp \cdots 1$
Let $x_1 = x_0 + y_0p^n$
Squaring both sides,
$x_1^2 = (x_0 + y_0p^n)_2 = x_0^2 + 2x_0y_0p^n + y_0^2p^{2n}$
$\Rightarrow x_1^2 = a + bp^n + 2x_0y_0p^n + y_0^2p^{2n}$ (By induction hypothesis)
$\Rightarrow x_1^2 = a + (b + 2x_0y_0)p^n + y_0^2p^{2n} = a + dp^{n+1} + y_0^2p^{2n}$ (By equation 1)
$\Rightarrow x_1^2 = a + p_{n+1}(d + y_0^2p^{n-1})$, (n-1) $\geq$ 0 $\forall$ n $\geq$ 1
$\Rightarrow x_1^2 \equiv_{n+1} a$
Hence proved. □

Theorem 16.3 *Let a be an odd integer. Then,$x^2 \equiv_2 a$ always has a solution.*
Proof: If a is odd, then $a \equiv_2$ 1 always. Any odd integer x satisfies this equation. □

Theorem 16.4 *Let a be an odd integer. Then, $x^2 \equiv_4 a$ has a solution iff $a \equiv_4$ 1.*
Proof: Since x is odd, let x = 2k + 1.
$x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1 \equiv_4$ 1 Since square of every odd integer is 1 modulo 4, hence $x^2 \equiv_4 a$ has solution only if $a \equiv_4$ 1. Note that every odd integer is a solution. □

Theorem 16.5 *Let a be an odd integer. Then, $x^2 \equiv_{2^n} a$, n $\geq$ 3 has a solution iff $a \equiv_8$ 1.*
Proof: Any solution must be odd since a is odd.
let x = 2k + 1
$\therefore x^2 - 1 = (2k + 1)^2 - 1 = 4k(k + 1)$
Since one of k and (k+1) must be even, $\therefore 8|(x^2 - 1)$ i.e. $x^2 \equiv_8$ 1.
Hence solution can exist only if $a \equiv_8$ 1. Now we prove existence of solution.
Proof by induction on n: Let $\equiv_8$ 1.
Induction Hypothesis: $x^2 \equiv_{2^n} a$, n $\geq$ 3 has a solution.
To prove: $x^2 \equiv_{2^{n+1}} a$, n $\geq$ 3 has a solution.
by induction Hypothesis, $x_0^2 = b2^n + a$ where x_0 and a are odd.

Also, $x_0 y \equiv_2 -b$ *has a unique solution since gcd(*x_0*,2) = 1 as* x_0 *is odd. Let that solution be* y_0*.*
$\therefore 2 | x_0 y_0 + b$ *. Let* $x_0 y_0 + b = 2j$
Now, consider $x_1 = x_0 + y_0 2^{n-1}$ *. Squaring, we get,*
$x_1^2 = x_0^2 + x_0 y_0 2^n + y_0^2 2^{2(n-1)} = a + (b + x_0 y_0) 2^n + y_0^2 2^{2(n-1)}$
$x_1^2 = a + j 2^{n+1} + y_0^2 2^{2(n-1)} \equiv_{2^{n+1}} a$ *if 2(n-1)* $\geq$ *n+1* $\Rightarrow n \geq 3$*.*
Hence Proved. □

Theorem 16.6 *Let* $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$ *be the prime factorization of n. For any* $a \perp n$*,* $x^2 = \equiv_n a$ *has a solution iff*

1. $\left\lfloor \begin{matrix} a \\ p_i \end{matrix} \right\rfloor$ *= 1* $\forall\ 1 \leq i \leq m$ *and*
2. $a \equiv_{2,4}$ *1 if* $k_0 \in$ *{1,2 } and* $a \equiv_8$ *1 if* $k \geq 3$*.*

Proof: $x^2 = \equiv_n$ a has a solution iff the following system of equations has a solution:

$$\begin{array}{ll} x^2 \equiv_2 a \bigvee x^2 \equiv_{2^2} a \bigvee \ldots \bigvee x^2 \equiv_{2^{k_0}} a & \cdots (0) \\ x^2 \equiv_{p_1^{k_1}} a & \cdots (1) \\ x^2 \equiv_{p_2^{k_2}} a & \cdots (2) \\ \vdots & \\ x^2 \equiv_{p_i^{k_i}} a & \cdots (i) \\ \vdots & \\ x^2 \equiv_{p_m^{k_m}} a & \cdots (m) \end{array}$$

Let equation i has solutions u_i and u_i' modulo $p_i^{k_i}$.

$$Now,\ x \quad = \quad \sum_{i=0}^{m} u_i . \frac{n}{p_i^{k_i}}\ satisfies\ all\ the\ above\ equations$$

Since a is a quadratic residue of p_i $\forall 1 \leq i \leq m$, hence $\left\lfloor \begin{matrix} a \\ p_i \end{matrix} \right\rfloor = 1$.
Proof of part (2) follows from theorem (16). □

Definition 16.1 Jacobi Symbol: *For any a and odd n, Jacobi symbol is defined as*

$$\left\rfloor \begin{matrix} a \\ n \end{matrix} \right\lfloor \quad = \quad \prod_{i=1}^{k} \left\lfloor \begin{matrix} a \\ p_i \end{matrix} \right\rfloor^{\alpha_i}$$
$$where\ n \quad = \quad \prod_{i=1}^{k} p_i^{\alpha_i}$$

Fact 16.7 $\left\rfloor \begin{matrix} a \\ n \end{matrix} \right\lfloor$ *= 1 does not imply that a is a quadratic residue of n.*

Fact 16.8 *a is a quadratic residue of n iff gcd(a, n) = 1 and a is a quadratic residue of of every prime factor of n.*

Chapter 17

The Jacobi Symbol

Definition 17.1 Jacobi Symbol: *For any a and odd n, Jacobi symbol is defined as*

$$
\begin{aligned}
\left(\frac{a}{n} \right) &= \prod_{i=1}^{k} \left[\frac{a}{p_i} \right]^{\alpha_i} \\
\textit{where, } n &= \prod_{i=1}^{k} p_i^{\alpha_i} \\
\textit{and } \left[\frac{a}{p} \right] & \textit{ is the Legendre Symbol.}
\end{aligned}
$$

The Jacobi symbol has many properties that make its use the easiest way to evaluate a Legendre symbol. Suppose m and n are positive odd integers, and a and b are any integers. Then the Jacobi symbol satisfies the following:

1. When n is a prime, the Jacobi symbol reduces to the Legendre symbol. Analogously to the Legendre symbol, the Jacobi symbol is commonly generalized to have value

   $$\left(\frac{m}{n} \right) = 0 \text{ if } m \mid n$$

   giving

   $$\left(\frac{n}{n} \right) = 0$$

   as a special case.

2. The Jacobi symbol is not defined for $n \leq 0$ or n even.

3. $\left(\frac{-1}{n} \right) = 1$ if $n \equiv_4 1$, and $\left(\frac{-1}{n} \right) = -1$ if $n \equiv_4 3$

4. $\left(\frac{a}{m} \right) \left(\frac{a}{n} \right) = \left(\frac{a}{mn} \right)$

5. $\left(\frac{a}{m} \right) \left(\frac{b}{m} \right) = \left(\frac{ab}{m} \right)$

6. if $a \equiv_m b$, then $\left(\frac{a}{m} \right) = \left(\frac{b}{m} \right)$

Theorem 17.1 *If n is odd then*

$$\left(\frac{-1}{n} \right) = (-1)^{\frac{n-1}{2}}$$

and

$$\left(\frac{2}{n} \right) = (-1)^{\frac{n^2-1}{8}}$$

Proof:

$$\begin{aligned}
\left(\frac{-1}{n} \right) &= \prod_{i=1}^{k} \left[\frac{-1}{p_i} \right] \text{ ...where, } n = \prod_{i=1}^{k} p_i \\
&= \prod_{i=1}^{k} (-1)^{\frac{p_i-1}{2}} \\
&= (-1)^{\sum_{i=1}^{k} \frac{p_i-1}{2}} \\
&= (-1)^{\frac{n-1}{2}} \text{ ...Using, } \frac{ab-1}{2} \equiv_2 \frac{a-1}{2} \frac{b-1}{2}
\end{aligned}$$

$$\begin{aligned}
\left(\frac{2}{n} \right) &= \prod_{i=1}^{k} \left[\frac{2}{p_i} \right] \\
&= \prod_{i=1}^{k} (-1)^{\frac{p_i^2-1}{8}} \\
&= (-1)^{\sum_{i=1}^{k} \frac{p_i^2-1}{8}} \\
&= (-1)^{\frac{n^2-1}{8}} \text{ ...Using, } \frac{a^2b^2-1}{8} \equiv_8 \frac{a^2-1}{8} \frac{b^2-1}{8}
\end{aligned}$$

□

Theorem 17.2 *If m and n are odd and $m \perp n$. then*

$$\left(\frac{m}{n} \right) \left(\frac{n}{m} \right) = (-1)^{\frac{m-1}{2} \frac{n-1}{2}}$$

Proof: Consider,

$$m = \prod_{i=1}^{k} p_i \text{ and } n = \prod_{j=1}^{l} q_j$$

Then, using the fact that $m \perp n$ otherwise there will be a p_i and q_j whose $\left\lfloor \begin{matrix} p_i \\ q_j \end{matrix} \right\rfloor = 0$, we get,

$$
\begin{aligned}
\left\rmoustache \begin{matrix} m \\ n \end{matrix} \right\lmoustache &= \prod_{i=1}^{k}\prod_{j=1}^{l} \left\lfloor \begin{matrix} p_i \\ q_j \end{matrix} \right\rfloor \\
&= \prod_{i=1}^{k}\prod_{j=1}^{l} \left\lfloor \begin{matrix} q_j \\ p_i \end{matrix} \right\rfloor (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} \\
&= \left\rmoustache \begin{matrix} n \\ m \end{matrix} \right\lmoustache (-1)^{\sum_i^k \sum_j^l \frac{p_i-1}{2}\frac{q_j-1}{2}} \\
&= \left\rmoustache \begin{matrix} n \\ m \end{matrix} \right\lmoustache (-1)^{(\sum_i^k \frac{p_i-1}{2})(\sum_j^l \frac{q_j-1}{2})} \\
&= \left\rmoustache \begin{matrix} n \\ m \end{matrix} \right\lmoustache (-1)^{(\frac{m-1}{2})(\frac{n-1}{2})} \quad \text{...Using, } \frac{ab-1}{2} \equiv_2 \frac{a-1}{2}\frac{b-1}{2}
\end{aligned}
$$

Multiplying both sides by $\left\rmoustache \begin{matrix} n \\ m \end{matrix} \right\lmoustache$ and Using $\left\rmoustache \begin{matrix} n \\ m \end{matrix} \right\lmoustache \left\rmoustache \begin{matrix} n \\ m \end{matrix} \right\lmoustache = 1$,

$$
\left\rmoustache \begin{matrix} m \\ n \end{matrix} \right\lmoustache \left\rmoustache \begin{matrix} n \\ m \end{matrix} \right\lmoustache = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}
$$

$\square$

Jacobi Algorithm Now, we will detail an algorithm to evaluate $\left\rmoustache \begin{matrix} a \\ n \end{matrix} \right\lmoustache$.
Suppose n is odd and $0 < a < n$.

$$
\begin{aligned}
a &= 2^k n' && \text{(where, } n' \text{ is odd)} \\
\left\rmoustache \begin{matrix} a \\ n \end{matrix} \right\lmoustache &= \left\rmoustache \begin{matrix} 2 \\ n \end{matrix} \right\lmoustache^k \left\rmoustache \begin{matrix} n' \\ n \end{matrix} \right\lmoustache && \left(\text{Using, } a \equiv_m b \Longrightarrow \left\rmoustache \begin{matrix} a \\ m \end{matrix} \right\lmoustache = \left\rmoustache \begin{matrix} b \\ m \end{matrix} \right\lmoustache\right) \\
&= (-1)^{k\frac{n^2-1}{8}} \left\rmoustache \begin{matrix} n' \\ n \end{matrix} \right\lmoustache \\
&= (-1)^{k\frac{n^2-1}{8}+\frac{n-1}{2}\frac{n'-1}{2}} \left\rmoustache \begin{matrix} n \\ n' \end{matrix} \right\lmoustache && \left(\text{Using, } \left\rmoustache \begin{matrix} m \\ n \end{matrix} \right\lmoustache \left\rmoustache \begin{matrix} n \\ m \end{matrix} \right\lmoustache = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\right)
\end{aligned}
$$

Now,

$$
\begin{aligned}
n &= qn' + a' && (0 < a' < n') \\
\left\rmoustache \begin{matrix} n \\ n' \end{matrix} \right\lmoustache &= \left\rmoustache \begin{matrix} a' \\ n' \end{matrix} \right\lmoustache && \left(\text{Using, } \left\rmoustache \begin{matrix} n' \\ n' \end{matrix} \right\lmoustache = 0\right)
\end{aligned}
$$

Hence we get,

$$
\left\rmoustache \begin{matrix} a \\ n \end{matrix} \right\lmoustache = (-1)^{k\frac{n^2-1}{8}+\frac{n-1}{2}\frac{n'-1}{2}} \left\rmoustache \begin{matrix} a' \\ n' \end{matrix} \right\lmoustache
$$

We started with (a, n) and arrived at a smaller pair (a', n').

Note:

1. $S = k\frac{n^2-1}{8} + \frac{n-1}{2}\frac{n'-1}{2}$ is odd iff

$$
\begin{matrix}
k \equiv_2 1 & \text{and} & \dfrac{n^2-1}{8} \equiv_2 1 \\
 & \text{XOR} & \\
\dfrac{n-1}{2} \equiv_2 1 & \text{and} & \dfrac{n-1}{2} \equiv_2 1
\end{matrix}
$$

2.

$$\left(\frac{0}{n} \right) = 1 \quad \text{if } n = 1$$
$$= 0 \quad \text{otherwise}$$

Here is how the algorithm works.

$$\begin{aligned} a_0 &= 2^{k_1} n_1 \\ n_0 &= q_1 n_1 + a_1 \\ a_1 &= 2^{k_2} n_2 \\ n_1 &= q_2 n_2 + a_2 \\ &\cdot \\ &\cdot \\ a_{m-1} &= 2^{k_m} n_m \\ n_{m-1} &= q_m n_m + a_m \end{aligned}$$

The moment when a_m becomes 0, the algorithm terminates.

Algorithm 17.1 The Jacobi Algorithm:

```
algorithm jacobi(a, n)
begin
  a <- a mod n;
  t <- 1;
  while (a<>0) do
  begin
    while (a is even) do
    begin
      a <- a div 2;
      if (n mod 8 = {3,5} ) then t <- -t;
    end
    swap (a,n);
    if (a mod 4 = 3  and  n mod 4 = 3) then t <- -t;
    a <- a mod n;
  end
  if (n=1) then return(t) else return(0);
end
```

Chapter 18

Elementary Algebraic Concepts

Definition 18.1 SemiGroup *A Semigroup $S =< S, \odot >$ is a set of elements S, and a binary operation called the semigroup product, such that*

- *S is closed under the Semigroup product $\odot$*
- *$\odot$ is Associative*

Definition 18.2 Left & Right Identities *An element $i \in S$ is a left identity if*

$$\forall a \in S, i \odot a = a$$

Similarly, an element $i \in S$ is a right identity if

$$\forall a \in S, a \odot i = a$$

Fact 18.1 *A semigroup cannot have distinct left and right identities.*

$$\begin{array}{rcll} i_L \odot i_R & = & i_L & \textit{Since } i_R \textit{ is the right identity} \\ i_L \odot i_R & = & i_R & \textit{Since } i_L \textit{ is the left identity} \\ \Rightarrow i_L & = & i_R & \end{array}$$

An element which is both a left & right identity is called an Identity.

Fact 18.2 *Identity elements if they exist are unique.*

From the above discussion it follows that a Semigroup can have more than one Left Identities, provided it doesnt have any Right Identities. But if there is even one Right Identity, all the Left Identities collapse into one. Same holds for the Right Identities too.

Definition 18.3 Monoid *A Semigroup with an Identity element is called a Monoid.*

A Monoid can be respresented as

$$\mu =< M, \odot, 1 >$$

where M is a set closed under $\odot$, $\odot$ is an associative binary operator, and 1 is the Identity.

- Set of all Postive Numbers with 1 as the Identity element under the Binary Operation Multiplication forms a Monoid
- Set of all Strings with Empty String as the Identity elemetns forms a monoid under Concatenation.

Definition 18.4 Inverse *Given a Monoid*

$$\mu =< M, \odot, 1 >$$

an element $a \in M$ is the left inverse of the element $b \in M$ if

$$a \odot b = 1$$

As is intuitive, b is the right inverse of a.

Theorem 18.3 *If every element of a monoid posseses a left inverse, then the left inverse is also the right inverse.*

Proof: Let b is the left inverse of a, and c is the left inverse of b

$$\Rightarrow b \odot a = 1, c \odot b = 1$$

Consider,

$$\begin{aligned} b \odot (a \odot b) &= (b \odot a) \odot b \quad \textit{Since } \odot \textit{ is Associative} \\ &= 1 \odot b \\ &= b \end{aligned}$$

$$\begin{aligned} c \odot (b \odot (a \odot b)) &= c \odot b \\ &= 1 \end{aligned}$$

However,

$$((c \odot b) \odot (a \odot b)) \quad = \quad a \odot b \quad \textit{[c is the LI of b]}$$

So, we have

$$\begin{aligned} 1 &= c \odot (b \odot (a \odot b)) \\ &= ((c \odot b) \odot (a \odot b)) \quad [\odot \textit{ is Associative]} \\ &= a \odot b \end{aligned}$$

$\Rightarrow$ b is the Right Inverse of a as well. □

Theorem 18.4 *If every element of a Monoid possesses a left inverse, then the inverses are unique.*

Proof: Lets prove this using Contradiction. Assume b and c are the two left inverses of a.

$$b \odot a = 1, c \odot a = 1$$

So, we have

$$\begin{aligned} 1 \odot b &= 1 \odot b \\ (b \odot a) \odot b &= (c \odot a) \odot b \quad \textit{[From above]} \\ b \odot (a \odot b) &= c \odot (a \odot b) \quad [\odot \textit{ - Associative]} \\ b \odot 1 &= c \odot 1 \quad \textit{[b is LI of a, so b is also RI of a]} \\ b &= c \end{aligned}$$

□

Definition 18.5 Group *A Monoid in which unique inverses are guaranteed is called a Group.*

Mathematically, a Group is defined as

$$G =< G, \odot, 1, ^{-1} >$$

where G is the set closed under the associative binary operator $\odot$, 1 is the identity element and $^{-1}$ is the unique inverse.
If $\odot$ is Commutative, then the group is called an Abelian Group.

Fact 18.5 *Given a group G,*

$$(a^{-1})^{-1} = a$$
$$(a \odot b)^{-1} = b^{-1} \odot a^{-1}$$

- Integers under Addition form a Group
- Z_p, set of integers from 1 to the prime p, forms a group under Multiplication (mod p)

Definition 18.6 Finite Group *If G is a finite group, then*

$$o(G) = |G|$$

Definition 18.7 Subgroup *For any group G, $H \subseteq G$ is a subgroup of G provided H is a group.*

1, G are the Trivial Subgroups of G

Fact 18.6 *If H is a subgroup of G, then*

$$\begin{array}{l} 1 \in H \\ a \in H \quad \Rightarrow \quad a_{-1} \in H \quad \textit{Since H is closed under } \odot \end{array}$$

Theorem 18.7 Lagrange's Theorem : *If G is a finite group and H is a subgroup of G, then*

$$o(H)|o(G)$$

Proof:

Claim 18.1 *The relation $\equiv_H \subseteq G \times G$ such that*

$$\begin{array}{rl} a \equiv_H b & \quad \textit{(read as: a is equivalent to b modulo H)} \\ \textit{iff} \quad ab^{-1} \in H & \end{array}$$

is an equivalence relation.

- **Reflexivity** $a \equiv_H a$ since, $a \odot a^{-1} = 1 \in H$
  Hence it is reflexive.
- **Symmetry**

$$\begin{array}{lccc} & a & \equiv_H & b \\ \Rightarrow & ab^{-1} & \in & H \\ \Rightarrow & (ab^{-1})^{-1} & \in & H \\ \Rightarrow & (b^{-1})^{-1}a^{-1} & \in & H \\ \Rightarrow & ba^{-1} & \in & H \\ \Rightarrow & b & \equiv_H & a \end{array}$$

- **Transitivity**

$$\begin{array}{rccl} & a & \equiv_H & b \\ \Rightarrow & ab^{-1} & \in & H \\ & b & \equiv_H & c \\ \Rightarrow & bc^{-1} & \in & H \\ \Rightarrow & (ab^{-1})(bc^{-1}) & \in & H \\ \Rightarrow & ac^{-1} & \in & H \\ \Rightarrow & a & \equiv_H & c \end{array}$$

Definition 18.8 Right Coset *For each $a \in G$, define H_a as the Right Coset of a, where*

$$H_a = \{h.a | h \in H\}$$

Definition 18.9 Equivalence Class *For any $a \in G$, define $[a]_H$ as the Equivalence Class of a, where*

$$[a]_H = \{a' | a \equiv_H a'\}$$

Claim 18.2 $H_a = [a]_H$

$\Longrightarrow H_a \subseteq [a]_H$, since for any $h \in H$,

$$\begin{array}{rccl} & a \odot (ha)^{-1} & = & a \odot a^{-1} \odot h^{-1} \\ & & = & h^{-1} \in H \\ \Rightarrow & a & \equiv_H & ha \\ \Rightarrow & ha & \in & [a]_H \end{array}$$

$\Longleftarrow [a]_H \subseteq H_a$,
For any $g \in [a]_H$,

$$\begin{array}{rccl} & a & \equiv_H & g \\ \Rightarrow & ag^{-1} & \in & H \\ \Rightarrow & (ag^{-1})^{-1} & \in & H \\ \Rightarrow & ga^{-1} & \in & H \\ \Rightarrow & (ga^{-1}) \odot a & \in & H \odot a \\ \Rightarrow & g & \in & H_a \end{array}$$

Hence, $H_a = [a]_H$

Claim 18.3 *For any $a, b \in H$, $H_a = H_b$ or $H_a \bigcap H_b = \phi$*

It follows from the fact that Equivalence Classes divide the set into disjoint partitions.

Claim 18.4 *There is a 1-1 correspondence between H_a and H_b, $\forall a.b \in G$*

$\vdash H_a = H_b$ is obvious.
otherwise $h_a \mapsto^f h_b$ for h ∈ H.
If f is not 1-1,

$$\begin{array}{rccl} & h_1 b & = & h_2 b \\ \Rightarrow & h_1 & = & h_2 \end{array}$$

Hence f is a bijection. Therefore, $|H_a| = |H_b|$
Since the group is entirely partitioned among equivalence classes which are disjoint, so if there are k equivalence classes,
$k \times o(H) = o(G)$ □

Corollary 18.8 *A group with Prime order can have only trivial subgroups.*

Remark 18.1 *Converse of Lagrange's Theorem is not true.*

Chapter 19

Sylow's Theorem

Given any element a of a finite group G. Consider the set of all powers of a, $a^0, a^1, \ldots$. Here $a^0 = 1$ is the identity element and a^1 is the element a itself.

Definition 19.1 *Order of an element of a group is defined to be* $\min_k$ *s.t.* $a^k = 1$.

Definition 19.2 *Define* $< a >= \{1, \ldots, a^{k-1}\}$. $< a >$ *is a cyclic subgroup of* G.

Definition 19.3 *For a subset* $H \subseteq G$ *define* $< H >= \{ab | a, b \in H \text{ or } < H >\}$. *If* $< H >= G$, *then* H *is called a set of generators for* G.

Corollary 19.1 *Every finite group of prime order is a cyclic group.*

Proof: Take any $a \in G, a \neq 1, O(< a >) | O(G)$, then, $O(< a >) = O(G)$. □

Corollary 19.2 *Every cyclic group is commutative.*

Sylow's Theorem

Lagrange's theorem only talks about the order of the subgroup of a group. It does not answer the reverse question of whether there exists a subgroup of a given order. Sylow's theorem answers this question albeit only for some values of the order of the subgroup.

Theorem 19.3 *If* p *is a prime and* $p^\alpha | O(G)$ *then* G *has a subgroup of order* p^α.

Proof: Assume $O(G) = n = p^\alpha m$ (note that p^α may not be the highest power of p in n.) Consider subsets of G of size p^α. The number of such subsets is

$$\binom{p^\alpha m}{p^\alpha} = \frac{p^\alpha m(p^\alpha m - 1) \ldots (p^\alpha m - p^\alpha + 1)}{p^\alpha (p^\alpha - 1) \ldots 1}. \tag{19.1}$$

Claim 19.1 *If* $p^\beta \| m$ *then* $p^\beta \| \binom{p^\alpha m}{p^\alpha}$.

Proof: For any γ, $p^\gamma \| (p^\alpha m - i)$ iff $p^\gamma \| (p^\alpha - i)$. All p^γ's cancel out leaving p^β which is then the highest power of p that divides $\binom{p^\alpha m}{p^\alpha}$. □ □

Definition 19.4 $\mathcal{M} = \{M \in G \ s.t. \ |M| = p^\alpha\}, \exists \beta \ s.t. \ p^\beta \| m$

Let us define a relation on the set $\mathcal{M}$. $M \sim N$ if $\exists g \in G$ s.t. $M = Ng$.

Claim 19.2 *The relation defined above is an equivalence relation.*

Proof: The relation as defined above is:

- Reflexive: take $g = 1$ in the relation above. Hence $M \sim M, \forall M$.
- Symmetric: If $M = Ng$, then, $\forall c \in N, \exists a \in M$ s.t. $a = cg$. Multiplying both sides by g^{-1}, $\forall a \in M, \exists c \in N$ s.t. $ag^{-1} = c$. Hence, $N = Mg^{-1}$, implies $N \sim M$.
- Transitive: If $M \sim N$ and $N \sim O$, then $\exists g, g'$ s.t. $, M = Ng$ and $N = Og'$. Hence, $M = Og'g$ and hence $M \sim O$.

□

Claim 19.3 $\exists$ *atleast one equivalence class* $[N]_\sim \in \mathcal{M}/\sim$ *s.t.* $p^{\beta+1} \not| \, |[N]_\sim|$.

Proof: Assume that every equivalence class is s.t. $p^{\beta+1} | \, |[M]_\sim|$ where $M \in \mathcal{M}$. We know that $|\mathcal{M}| = \binom{p^\alpha m}{p^\alpha}$. This implies that $p^{\beta+1} | \, |\mathcal{M}| = \binom{p^\alpha m}{p^\alpha}$. Choose $[N]_\sim = \{M_1, \ldots, M_K\}$Z s.t. $p^{\beta+1} \not| |[N]_\sim|$. Obviously, $\forall M_i, M_j \in [N]_\sim, \exists g \in G$ s.t. $M_i = M_j g$. Let $H = \{g \in G | M_1 = M_1 g\}$. □

Claim 19.4 *H is a subgroup of G.*

Proof: We show that H is closed, has the identity element and elements in H also have their inverses in H.

- If $g_1, g_2 \in H$, then, $M_1 = M_1 g_2 = (M_1 g_1) g_2 = M_1 (g_1 g_2)$. Hence H is closed under $\cdot$.
- The element 1 is the identity element of the group H.
- For any $g \in G$, the inverse of g in G also belongs to H. For any element $a \in M_1, \exists c \in M_1$ s.t. $a = cg$. As The mapping from M_1 to M_1 is one-to-one $\forall c \in M_1, \exists a \in M_1, $ s.t. $c = ag^{-1}$. Hence $g^{-1} \in H$.

Hence H is a subgroup of G. □

Theorem 19.4 *$kO(H) = O(G)$.*

Proof: We construct a bijection between $[N]_\sim$ and the set of right cosets of G/H of H. By construction of H we get the equivalence:

$$(Ha = Hb) \equiv (ab^{-1} \in H) \equiv (M_1 ab^{-1} = M_1) \equiv (M_1 a = M_1 b), \forall a, b \in G. \tag{19.2}$$

That is whenever a and b are in the same right coset of H (or their cosets are equal, respectively) they form the same $M_1 a = m_! b$, name it N. $N \in [N]_\sim$ because $Nb^{-1} = M_1$. Hence, $N \sim M_1$. So $Ha \to M_1 a, \forall a \in G$, defines a mapping from G/H to $[N]_\sim$. Since $N \in [N]_\sim$, N is some M_j, $j \in 1, \ldots, k$. Conversely, each M_j is of the form $M_1 a$ for some $a \in G$ by definition. So the mapping $Ha \to M_1 a, \forall a \in G$ is in fact a bijection. □

Claim 19.5 $O(H) = p^\alpha$.

Proof:

$$\begin{aligned} p^\beta &\parallel m && (19.3)\\ \implies p^{\alpha+\beta} &\parallel p^\alpha m && (19.4)\\ &= kO(H). && (19.5)\end{aligned}$$

As

$$p^{\beta+1} \not| k \quad (19.6)$$

so

$$p^\alpha | O(H). \quad (19.7)$$

This implies $O(H) \geq p^\alpha$.

$|M_1| = p^\alpha$. Consider any $a \in M_1$. For any $h, h' \in H$,

$$\begin{aligned} ah &\in M_1 && (19.8)\\ ah' &\in M_1. && (19.9)\end{aligned}$$

Also $ah = ah'$ implies that $h = h'$. Therefore M_1 has $\geq O(H)$ distinct elements. Thus, $O(H) = p^\alpha$. □

Rings and Fields

Definition 19.5 *A ring* $< R, +, \cdot, 0, 1 >$ *s.t.*

1. $< R, +, 0 >$ *is an abelian group.*
2. $< R, \cdot, 1 >$ *is a monoid.*
3. $\cdot$ *distributes over* $+$.

For eg. Integers form a ring under addition and multiplication.

Definition 19.6 *R is a commutative ring if* $\cdot$ *is commutative. For eg.* 2×2 *non-singular matrices over reals form a ring but not a commutative ring.*

Definition 19.7 *R is a field if* $< R - \{0\}, \cdot, 1 >$ *is an abelian group. For eg.* $\mathbf{Z}_p$ *is a field for any prime p.*

Theorem 19.5 $\mathbf{Z}_m$ *for any composite m is not a field.*

Proof: If m is not a prime then $\exists a \in \mathbf{Z}_m$ s.t. $\gcd(a, m) \neq 1$. This implies that $ax \equiv_m 1$ has no solution, which means that $\not\exists b \in \mathbf{Z}_m$ s.t. $ab \equiv_m 1$. □

Chapter 20

Finite Abelian Groups & Dirichlet Characters

20.1 Introduction

Definition 20.1 *An Abelian group is a set G with a binary operation $\circ$ satisfying the following conditions:*

- *For all $a, b, c \in G$, we have, $a \circ (b \circ c) = (a \circ b) \circ c$ (the associative law)*
- *There is an element $e \in G$ s.t. $a \circ e = a$ for all $a \in G$*
- *For any $a \in G$ there exists $b \in G$ such that $a \circ b = e$(existence of an inverse)*
- *For all $a, b \in G$, we have, $a \circ b = b \circ a$(the commutative law)*

A finite abelian group $G' \subseteq G$ where G is finite but not necessarily abelian.
Since $a \in G$, $order(a)$ exists.

$$a^{order(a)} = 1 \in G'$$

Definition 20.2 *Define $ind(a, G')$ as the smallest positive integer such that*

$$a^{ind(a,G')} \in G'$$

Then, $1 \leq ind(a, G') \leq order(a)$

Theorem 20.1 *Let $G' \subseteq G$ be a subgroup of a finite abelian group G. Let $a \in G - G'$ and $h = ind(a, G')$*

$$G'' = \{xa^k | x \in G', 0 \leq k < h\}$$

Then G" is a subgroup of G s.t.
(i) $G' \subset G''$
(ii) $|G"| = h|G'|$

Proof: (i) Consider $xa^j * ya^k$ where $x, y \in G', 0 \leq j, k < h$

$$\begin{array}{rr} Case1: & j + k < h \Rightarrow xa^j * ya^k = xya^{j+k} \in G'' \\ Case2: & j + k \geq h \Rightarrow a^{j+k} \in G' \subset G'' \\ & But, a^{j+k} = a^h a^i \, where 0 \leq h < i \\ & Now, a^h = 1 \, and \, a^i \in G' \end{array}$$

Hence G" is closed under *

Now we need to show that xa^k has an inverse in G"
Let the inverse be $x^{-1}a^{n-k}$
This is something of the form xa^{h+i} where $0 \leq i < h$
i.e. $(xa^h)a^i \in G''$
Hence (i) proved

(ii) For each element $a \in G'$ we can get at most h elements in G'' i.e.

$$a^0, a^1, ..., a^{h-1}$$

If $|G'| = m$ then all we need to show is that the resulting hm elements in G'' are distinct. We prove this by contradiction. Assume

$$xa^j = ya^k$$

$$\Rightarrow x = ya^{k-j}$$

Without loss of generality, we assume, $h > k \geq j$. Then

$$xy^{-1} = a^{k-j} \in G'$$

We know that $k - j < h$ and h is the smallest positive integer s.t. $a^h \in G'$

$$\Rightarrow k - j = 0$$

$$\Rightarrow x = y$$

Hence, $|G"| = h|G'|$ □

20.2 Characters of Finite Abelian Groups

Definition 20.3 *A character is a complex valued function which is multiplicative.*

Complex Valued: f maps each element in a group to a complex number.
Multiplicative: $f(a)f(b) = f(ab)$ and $\exists c \in G\colon f(c) \neq 0$

Fact 20.2 *Every group has a character $f(a) = 1 \forall a \in G$ called the Principal Character*

Theorem 20.3 *If f is a character of a finite abelian group G then $f(e) = 1$ (where e is the identity element) and each $f(a), a \in G$ is a root of unity.*

Proof: For some $c \in G$

$$f(c) \neq 0$$

$$\Rightarrow f(ce) = f(c) = f(c)f(e)$$

$$\Rightarrow f(e) = 1$$

Now, consider any $a \in G, order(a) = n$

$$a^n \equiv e$$

$$f(a^n) = f(a)^n = 1 = f(e)$$

Hence, every f(a) is a root of unity. □

Theorem 20.4 *A finite abelian group of order n has exactly n distinct characters.*

Proof:

$$\vdash \{e\} = G_0 \subset G_1 \subset ...... \subset G_n = G$$

$$G_{i+1} = \langle G_i; a_{i+1} \rangle, a_{i+1} \ni G_i$$

Proof by Induction follows:

Base Case: {e} has exactly one character.

Induction Step:
Assume G_i has $|G_i|$ characters.
Elements of G_{i+1} are given by $xa_{i+1}^k, x \in G_i$

Let f_i be a character of G_i
We now define $\hat{f}_i$ as

$$\hat{f}_i(x) = f_i(x) \forall x \in G_i$$

$$\begin{aligned} \hat{f}_i(xa_{i+1}^k) &= \hat{f}_i(x)\hat{f}_i(a_{i+1})^k \\ &= f_i(x)\hat{f}_i(a_{i+1})^k \end{aligned}$$

Let $h = ind(a_{i+1}, G_i$

$$\Rightarrow a_{i+1}^h = c \in G_i$$

Define $\hat{f}_i(a_{i+1})$ as the h^{th} root of $f_i(c)$
(Note: $f(c) \neq 0$ since all $f_i(c)$ are roots of unity.)

$\hat{f}_i(a_{i+1})$ is one of h possible roots of $f_i(c)$
Hence there are at most h extensions for each character of G_i

Claim 20.1 *$\hat{f}_i$(defined using one of the h^{th} roots of $f(c)$) is a character of G_{i+1}*

Claim 20.2 *There are h possible extensions of each character of G_i*
Outline of Proof *No two extensions $\hat{f}_i$ and $\hat{g}_i$ can be identical since that would mean f_i and g_i are identical.*

Hence there are exactly $h|G_i| = |G_{i+1}|$ characters of G_{i+1}. □

Definition 20.4 *If f and g are characters of a finite abelian group G then*

$$(f * g)(a) = f(a)g(a)$$

Theorem 20.5 *For any finite abelian group G, define*

$$\hat{G} = \{f | f\, is\, a\, character\, of\, G\}$$

then $\langle \hat{G}, *, f_1 \rangle$ is a finite abelian group (f_1 is the principal character) where $f^{-1} \equiv \frac{1}{f}$

Proof: If g is the inverse of f then $g(a) = \frac{1}{f(a)}$

$$\Rightarrow f^{-1}(a) = f(a^{-1}) = \frac{1}{f(a)}$$

Since G is abelian, $\hat{G}$ is abelian with the same order. □

Definition 20.5 *Given*

$$G = \{a_1, a_2, ..., a_n\}$$
$$\hat{G} = \{f_1, f_2, ..., fn\}$$

define $A(G)$ *as*

$$A(G) = [a_{ij}] = [f_i(a_j)]$$

Theorem 20.6 *The sum of the elements in row* i *of* A *is given by*

$$\begin{aligned} \textstyle\sum_{r=1}^{n} f_i(a_r) &= n \quad if\, i = 1 \\ &= 0 \quad otherwise \end{aligned}$$

Proof: If $i = 1, f_i = f_1$, the principal character, then

$$\sum_{r=1}^{n} f_1(a_r) = 1 * n = n$$

If $i \neq 1, \exists b \in G | f_i(b) \neq 1$ otherwise $f_i = f_1$

$$S = \sum_{r=1}^{n} f_i(a_r) = \sum_{r=1}^{n} f_i(ba_r) = f_i(b)S$$
$$\Rightarrow S(1 - f_i(b)) = 0$$

Since $f_1(b) \neq 1, S = 0$

□

Corollary 20.7 *The sum of the elements in column* j *of* A *is given by*

$$\begin{aligned} \textstyle\sum_{r=1}^{n} f_r(a_j) &= n \quad if\, a_j = e \\ &= 0 \quad otherwise \end{aligned}$$

Definition 20.6 *Define* A^* *as the conjugate transpose of* A.

$$A^* = [a^*_{ij}] = [\bar{f}_j(a_i)]$$

Theorem 20.8 $AA^* = nI$

Proof: $B = AA^*$

$$\begin{aligned} b_{ij} &= \textstyle\sum_{r=1}^{n} f_i(a_r)\bar{f}_j(a_r) \\ &= \textstyle\sum_{r=1}^{n} (f_i * \bar{f}_j)(a_r) \\ &= \textstyle\sum_{r=1}^{n} (f_k)(a_r) \end{aligned}$$

where

$$f_k = \frac{f_i}{f_j} = 1 \quad iff\, i = j$$

$$\begin{aligned} b_{ij} &= n \quad if\, i = j \\ &= 0 \quad otherwise \end{aligned}$$

$$\Rightarrow B = nI$$

□

Corollary 20.9 $A^*A = nI$

20.3 Characters of a Finite Abelian Group

- Every finite abelian group has as many characters as the order of the group.
- A character is a complex valued multiplicative function.
- The characters of a finite abelian group form a finite abelian group of the same order with the principal character as the identity element.
- For each character f and $a \in G$, $f(a)$ is a root of unity.
- $A(G) = [a_{ij}] = [f_i(a_j)]$
- A has an inverse A^* i.e. $AA^* = nI$
- Orthogonality Properties

  1. $$\begin{aligned} \sum_{r=1}^{n} f_i(a_r) &= n \quad if\, f_i\, is\, the\, principal \\ &= 0 \quad otherwise \end{aligned}$$

  2. $$\begin{aligned} \sum_{r=1}^{n} f_r(a_j) &= n \quad if\, a_j = e \\ &= 0 \quad otherwise \end{aligned}$$

20.4 Dirichlet Characters

For any integer m, ϕ_m is a finite abelian group under multiplication.

Definition 20.7 *S is called a* **Reduced Residue System** *if* $|S| = \phi(m)$ *and* $S \equiv \phi_m$ *Any* $\phi(m)$ *numbers that are mutually congruent modulo m form a Reduced Residue System.*

Fact 20.10 *Each S has* $\phi(m)$ *characters.*

For any character f,

$$a \equiv_m b \Rightarrow f(a) = f(b)$$

Definition 20.8 *For any reduced residue system modulo m, S and character f, we define a* **Dirichlet Character**, $\chi_f(n)$ *as*

$$\begin{aligned} \chi_f(n) = \quad & f(n) \quad if\, n \perp m \\ & 0 \quad otherwise \end{aligned}$$

Fact 20.11 *There are* $\phi(m)$ *Dirichlet Characters.*

Definition 20.9 *The Dirichlet Character corresponding to* f_1 *is called the Principal Dirichlet Character.*

Theorem 20.12 *The* $\phi(m)$ *Dirichlet Characters are:*

1. *multiplicative*
2. *periodic*
3. *Let* f *be any function s.t.* $f(n) = \chi(n)$ *if* $m \perp n$*, then* f *is a character of the group.*

Proof:

1. multiplicative - follows from multiplicativity of characters.
2. periodic - follows from $a \equiv_m b \Rightarrow f(a) = f(b)$

$\square$

Theorem 20.13 *The conjugate of each Dirichlet Character is also a Dirichlet Character.*

$$\sum_{r=1}^{\phi(m)} \chi_r(k)\bar{\chi}_r(l) = \begin{array}{ll} \phi(m) & if k \equiv_m l, l \perp m \\ 0 & otherwise \end{array}$$

The proof follows from orthogonality properties of characters.

Before we move on to the next theorem we need to study **Abel's Identity**.

Definition 20.10 *An* **arithmetical function** *is a real/complex valued function on positive integers.*

Theorem 20.14 **Abel's Identity***: Let $a(n)$ be an arithmetical function and let*

$$A(x) = \sum_{n \le x} a(n)$$

where $A(x) = 0$ if $x < 1$.If f is a function with a continuous derivative on the interval $[y, z]$, $0 < y < z$,then

$$\sum_{y<n\le z} a(n)f(n) = A(z)f(z) - A(y)f(y) - \int_y^z A(t)f'(t)dt$$

Analysis: $a(n)$ is a set of impulses.
$A(n)$ is a step function.
$f'(t)$ is continuous $\Rightarrow f(t)$ is continuous.

Proof: Let $k = \lfloor y \rfloor$ and $m = \lfloor z \rfloor$, then

$$\begin{aligned} \sum_{y<n\le z} a(n)f(n) &= \sum_{n=k+1}^{m} a(n)f(n) \\ &= \sum_{n=k+1}^{m} [A(n) - A(n-1)]f(n) \\ &= \sum_{n=k+1}^{m} A(n)f(n) - \sum_{n=k}^{m-1} A(n)f(n+1) \\ &= \sum_{n=k+1}^{m-1} A(n)(f(n) - f(n+1)) + A(m)f(m) - A(k)f(k+1) \\ &= \sum_{n=k+1}^{m-1} A(n)(f(n) - f(n+1)) + (A(z)f(z) - \int_m^z A(t)f'(t)dt) - (A(y)f(y) + \int_y^{k+1} A(t)f'(t)dt) \end{aligned}$$

Now

$$f(n+1) - f(n) = \int_n^{n+1} f'(t)dt$$

$$\begin{aligned} \sum_{n=k+1}^{m-1} A(n)(f(n) - f(n+1)) &= -\sum_{n=k+1}^{m-1} A(n) \int_n^{n+1} f'(t)dt \\ &= -\int_{k+1}^{m} A(t)f'(t)dt \end{aligned}$$

Substituting above, we get

$$\sum_{y<n\leq z} a(n)f(n) = A(z)f(z) - A(y)f(y) - \int_y^z f'(t)dt$$

Since limits on integrals cover this range. □

We now proceed to the next theorem.

Theorem 20.15 *Let χ be a non-principal Dirichlet character modulo k and let f be a non-negative valued function with a continuous negative derivative $f'(x)$ for all $x > x_0$. Then for all $x, y : x_0 \leq x \leq y$*

1.
$$\sum_{x<n<y} \chi(n)f(n) = O(f(x))$$

2. *If $lim_{x\to\infty}$, then $\sum_{n=1}^{\infty} \chi(n)f(n)$ converges and for $x \geq x_0$*

$$\sum_{n\leq x} \chi(n)f(n) = \sum_{n=1}^{\infty} \chi(n)f(n) + O(f(x))$$

Proof:

1. χ is an arithmetical function, hence *Abel's Identity* holds.

$$A(x) = \sum_{n\leq x} \chi(n)$$

From orthogonality properties,

$$A(k) = \sum_{n=1}^{k} \chi(n) = 0$$

$\chi(n)$ is periodic

$$\Rightarrow A(mk) = A(k) = 0$$

Now, $|A(x)| \leq \phi(k)$ for all x

$$\Rightarrow A(x) = O(1)$$

From Abel's Identity,

$$\begin{aligned} \textstyle\sum_{x<n\leq y} \chi(n)f(n) &= f(y)A(y) - f(x)A(x) - \textstyle\int_x^y \mathbb{A}(t)f'(t)dt \\ &= O(f(y)) + O(f(x)) + O(\textstyle\int) \\ &= O(f(x)) \end{aligned}$$

2. For $x \geq x_0$

$$\begin{aligned} \textstyle\sum_{n=1}^{\infty} \chi(n)f(n) &= \textstyle\sum_{n\leq x} \chi(n)f(n) + lim_{y\to\infty} \textstyle\sum_{x<n\leq y} \chi(n)f(n) \\ &= \textstyle\sum_{n\leq x} \chi(n)f(n) + O(f(x)) \end{aligned}$$

Hence Proved. □

Chapter 21

Dirichlet Products

Definition 21.1 *The Mobius Function denoted by μ is defined as:*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1. \\ (-1)^k & \text{if } n = \prod_{i=1}^{k} p_i \text{ where } i \neq j \Longrightarrow p_i \neq p_j. \\ 0 & \text{if } n \text{ contains a square.} \end{cases} \tag{21.1}$$

Fact 21.1 *For $n \geq 1$, the function $\mu(n)$ is multiplicative and*

$$\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 0 & \text{if } n > 1 \\ 1 & \text{if } n = 1 \end{cases} \tag{21.2}$$

Proof: Since,

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{i \neq j} \mu(p_i p_j) + \ldots \mu(p_1 p_2 \ldots p_k) \\ &= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \ldots + \binom{k}{k}(-1)^k. \\ &= (1-1)^k. \\ &= 0. \end{aligned}$$

□

Theorem 21.2 *For $n \geq 1$, $\phi(n) = \sum_{d|n} \mu(d) \left(\frac{d}{n}\right)$.*

Proof:

$$\begin{aligned}
\text{Since } \phi(n) &= \sum_{k=1}^{n} 1 \\
&= \sum_{k=1} \lfloor \frac{1}{gcd(k,n)} \rfloor \\
&= \sum_{d|gcd(k,n)} \mu(d) = \sum_{d|n} \sum_{d|k}^{n} \mu(d) \\
&= \sum_{d|n} \mu(d) \sum_{l=1}^{n/d} (1) = \sum_{d|n} \mu(d)(\frac{n}{d}).
\end{aligned}$$

□

Definition 21.2 *If f and g are arithmetical functions then their Dirichlet product or convolution is the function $h = f \star g$ where*

$$h(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{d.e=n} f(d)g(e) \tag{21.3}$$

Fact 21.3 *h is also arithmetical.*

Fact 21.4 *$\star$ is both commutative and associative.*

Proof: Consider $f \star (g \star h)$ and let $i = g \star h$. Then,

$$\begin{aligned}
(f \star i)n &= \sum_{a.b=n} f(a)i(b) \\
&= \sum_{a.b=n} f(a) \sum_{c.d=b} g(e)h(d) \\
&= \sum_{a.c.d=n} f(a)g(c)h(d) = (f \star g) \star h.
\end{aligned}$$

□

Fact 21.5 *$I(n) = \left\lfloor \frac{1}{n} \right\rfloor$ is the identity function for $\star$ and*

$$f \star I = f = I \star f.$$

Fact 21.6 *Let f be arithmetical with $f(1) \neq 0$. Then there exists unique f^{-1} given by,*

$$\begin{aligned}
f^{-1}(1) &= \frac{1}{f(1)} \\
f^{-1}(n) &= \frac{-1}{f(n)} \sum_{d|n,d<n} f\left(\frac{n}{d}\right) f^{-1}(d) \text{ for } n > 1
\end{aligned}$$

Proof: We derive f^{-1} in this proof.

$$\begin{aligned}
\text{Since } f \star f^{-1} &= I. \\
\text{Which implies, } f(1)f^{-1}(1) &= 1. \\
\text{Hence } f^{-1}(1) &= \frac{1}{f(1)}. \\
\text{Also for any } n \neq 1, \sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) &= 0. \\
\text{Thus, } \sum_{d|n, d<n} f\left(\frac{n}{d}\right) f^{-1}(d) &= -f(1)f^{-1}(n). \\
\text{Hence, } f^{-1}(n) &= \frac{-1}{f(n)} \sum_{d|n, d<n} f\left(\frac{n}{d}\right) f^{-1}(d).
\end{aligned}$$

The group of these functions is abelian and hence, $(f \star g)^{-1} = f^{-1} \star g^{-1}$. Also the inverse of the Mobius function μ is μ itself.

□

Theorem 21.7 *Mobius Inversion Formula:*

$$f(n) = \sum_{d|n} g(d) \ \textit{iff}\ g(n) = \sum_{d|n} f(d)\, \mu\left(\frac{n}{d}\right) = (f \star \mu)n.$$

Definition 21.3 *Mangoldt Function* Λ *is defined as:*

$$\Lambda(n) = \begin{cases} log(p) \ \text{if } n = p^m \text{ for some prime } p \\ 0 \ \text{otherwise} \end{cases}$$

Fact 21.8 *If* $n \geq 1$, $log(n) = \sum_{d|n} \Lambda(d)$.

Proof: if $n = \prod_{i=1}^{k} (p_i^{\alpha_i})$, then

$$\begin{aligned}
log(n) &= \sum_{i=1}^{k} \alpha_i log(p_i) \\
&= \sum_{i=1}^{k} \sum_{j=1}^{\alpha_i} \Lambda(p_i^j) \\
&= \sum_{d|n} \Lambda(d).
\end{aligned}$$

□

Theorem 21.9 *For* $n \geq 1$,

$$\Lambda(n) = \sum_{d|n} \mu(d) log\left(\frac{n}{d}\right) = -\sum_{d|n} \mu(d) log(d).$$

Proof:

$$\begin{aligned}
\text{Since } log(n) &= \sum_{d|n} \Lambda(d). \\
\text{Using the Mobius Inversion Formula, } \Lambda(n) &= \sum_{d|n} log(d)\mu\left(\frac{n}{d}\right) \\
&= \sum_{d|n} \mu(d)(log(n) - log(d)) \\
&= log(n)\sum_{d|n}\mu(d) - \sum_{d|n}\mu(d)log(d) \\
&= 0.
\end{aligned}$$

□

Generalized Convolutions

Let f be a real or complex valued function on the $[0, \infty)$ with $F(x) = 0$ for $0 < x < 1$. Let a be an arithmetical function s.t.

$$(a \circ F)(x) = \sum_{n \le x} a(n)F\left(\frac{x}{n}\right) \tag{21.4}$$

If F is arithmetical then $a \circ F = a \star F$.

Theorem 21.10 *If a and b are arithemtical and F is as defined above, then*

$$a \circ (b \circ F) = (a \star b) \circ F \tag{21.5}$$

.

Proof:

$$\begin{aligned}
\{a \circ (b \circ F)\}(x) &= \sum_{n \le x} a(n) \sum_{m \le x} \frac{x}{n} b(x) F\left(\frac{x}{mn}\right). && (21.6)\\
&= \sum_{mn \le x} a(n)b(m)F\left(\frac{x}{mn}\right). && (21.7)\\
&= \{(a \star b) \circ F(x)\}. && (21.8)
\end{aligned}$$

□

Fact 21.11 *$I(n)$ is the identity function for $\circ$.*

Proof: $(I \circ F)(x) = \sum_{n \le x} F\left(\frac{x}{n}\right) = F(x).$ □

Generalized Inversion

If a has a Dirichlet inverse a^{-1}, then

$$\begin{aligned}
G(x) &= \sum_{n \le x} a(n)F\left(\frac{x}{n}\right), \text{ where } G = a \circ F. \\
\text{iff } F(x) &= \sum_{n \le x} a^{-1}(n)G\left(\frac{x}{n}\right), \text{ where } F = a^{-1} \circ G.
\end{aligned}$$

Also if $G = a \circ F$, then $a^{-1} \circ G = a^{-1} \circ (a \circ F) = (a^{-1} \star a) \circ F = I \circ F \circ F$.

Partial Sums of Dirichlet Products

Theorem 21.12 *If $h = f \star g$, let*

$$\begin{aligned} H(x) &= \sum_{n \le x} h(n) \\ G(x) &= \sum_{n \le x} g(n) \\ \textit{and } F(x) &= \sum_{n \le x} f(n). \\ \textit{Then } H(x) &= \sum_{n \le x} f(n) G\left(\frac{x}{n}\right) \\ &= \sum_{n \le x} g(n) F\left(\frac{x}{n}\right). \end{aligned}$$

Definition 21.4

$$\textit{Let } U(x) = \begin{cases} 0 & \textit{if } 0 < x < 1; \\ 1 & \textit{if } x \ge 1. \end{cases} \tag{21.9}$$

Proof: Let $F = f \circ U$, $G = g \circ U$ and $H = h \circ U$. Therefore,

$$\begin{aligned} f \circ G &= f \circ (g \circ U). \\ &= (f \star g) \circ U \text{ (from Theorem 1.10)}. \\ &= (g \star f) \circ U \text{ (using commutativity)}. \\ &= h \circ U. \end{aligned}$$

The proof then follows from the definition of F, G and H above. □

Corollary 21.1 *If $F(x) = \sum_{n \le x} f(n)$ then,*

$$\sum_{n \le x} \sum_{d|n} f(d) = \sum_{n \le x} f(n) \lfloor \frac{x}{n} \rfloor = \sum_{n \le x} F\left(\frac{x}{n}\right).$$

Proof:

$$\begin{aligned} \sum_{n \le x} \sum_{d|n} f(d) &= \sum_{n \le x} \sum_{d|n} f(d) g\left(\frac{n}{d}\right). \\ &= \sum_{n \le x} (f \star g) \\ &= \sum_{n \le x} f(n) G\left(\frac{x}{n}\right) \\ &= \sum_{n \le x} g(n) F\left(\frac{x}{n}\right) \\ &= \sum_{n \le x} F\left(\frac{x}{n}\right). \end{aligned}$$

□

Chapter 22

Primes are in P

Overview

In this lecture we study the recent result from Manindra Agrawal, Neeraj Kayal and Nitin Saxena of the Indian Institute of Technology, Kanpur. The paper is titled "Primes is in P", and solves this longstanding open problem.

The paper presents a polynomial time algorithm for recognizing prime numbers, solving a longstanding open problem in Complexity Theory, and passing a milestone in the centuries-old journey towards understanding prime numbers.

We describe below a version of the algorithm of Agrawal, Kayal and Saxena, and sketch a proof of correctness.

Problem Description and Methodology

We want a polynomial-time method to determine if a given number n is prime, that is, a method that terminates after performing $O((\log n)^c)$ steps of computation. To put the problem in perspective, the previous best algorithm for primality testing is due to Adleman, Pomerane and Rumely and runs in $(logn)^{logloglogn}$ time, which as we can see is not polynomial in the length of the number n. Before describing the algorithm, we look at an identity for primeness.

Lemma 22.1 *(a) If n is prime, then $(X - a)^n \equiv_n X^n - a$.*

(b) If $\gcd(a, n) = 1$ and n is composite, then $(X - a)^n \not\equiv_n X^n - a$.

Proof: (Sketch)

(a) If n is prime $\binom{n}{i} \equiv_n 0$ for $i = 1, 2, \ldots, n - 1$ and $a^n \equiv_n a$.

(b) If n is composite and p is a prime factor of n, then the coefficient of X^p in $(X - a)^n$, is $\binom{n}{p}(-a)^{n-p} \not\equiv_n 0$.

□

This lemma leads naturally to the algorithm as described in Fig. 22.1..

If $(X - 1)^n \equiv_n X^n - 1$, then n is prime, otherwise it is composite.

Figure 22.1: A primality testing algorithm

This algorithm classifies numbers correctly as prime and composite; unfortunately, it cannot be implemented efficiently. There are two difficulties. First, the straightforward method for computing the polynomial $(X-1)^n$, requires $n-1$ multiplications, and we are allowing ourselves only $O((\log n)^c)$ time. This is not a serious problem. It is well-known that one can compute powers more efficiently by repeated squaring (see Figure 22.2). Interestingly, the use of repeated squaring for computing powers seems to have originated in India, but in the

> If n is a k-bit number, then for $i = 0, 1, 2, \ldots, k$, compute $b_i \equiv_n (X-1)^{2^i}$ by repeated squaring, starting from $b_0 = X - 1$. Let $n = \sum_{j=0}^{k} \epsilon_i 2^i$, $\epsilon_i \in \{0,1\}$ be the binary expansion of n. Then, $(X-1)^n = \prod_{i=0}^{k} b_i^{\epsilon_i}$.

Figure 22.2: Powering by repeated squaring

absence of email, it took some time for the word to get around. The procedure is reported to have existed as early as 200 B.C.

The second problem with the algorithm of Figure 22.1, and this is more serious, is that the polynomial $(X-a)^n$ has too many coefficients, potentially $n+1$, and computing such a polynomial even by the repeated squaring, is not feasible in $O((\log n)^c)$ steps. The key idea in the new primality test is to perform computations modulo a polynomial of small degree. This way, the number of coefficients in the polynomial stays small.

> **Input:** A integer $n \geq 2$.
>
> **Step 1:** If n is of the form a^b, for integers $a, b \geq 2$, then n is composite.
>
> **Step 2:** Choose the smallest prime r, so that r does not divide n, and the order of n modulo r is divisible by a prime $q \geq \lfloor 2\sqrt{r} \log n \rfloor + 2$. Let $\ell = \lfloor 2\sqrt{r} \log n \rfloor + 1$.
>
> **Step 3:** For $a = 2, 3, \ldots, \ell$, if a divides n, then n is composite.
>
> **Step 4:** For $a = 1, 2, \ldots, \ell$, if $(X-a)^n \not\equiv_{X^r-1,n} X^n - a$, then n is composite.
>
> **Step 5:** If n has not been declared composite by the earlier steps, then n is prime.

Figure 22.3: The new primality testing algorithm PTA of Agrawal, Kayal and Saxena

Definition 22.1 *$f(x) \equiv_{X^r-1,n} g(x)$ if the coefficients of the respective terms of $f(x)$ and $g(x)$ are equal mod n and the degree of the terms are equated mod r.*

To implement Step 2 of the procedure described in Fig. 22.3, we try all primes, starting from 2, one after the other. If at any stage we discover a non-trivial divisor of n, we declare that n is composite. It can be shown that for all large n, the prime r in Step 2, can be chosen to be $O((\log n)^6)$. We refer the reader to the original paper for a justification of this claim, which is based on a theorem due to Fouvry (1985). Assuming this, it is straightforward to check that this algorithm runs in polynomial-time. We will concentrate only on showing that this algorithm is correct.

Proof of Correctness

It is easy to verify, using Lemma 22.1, that if n is prime, this algorithm will never declare that it is composite. So, we only need to argue that composite numbers are not declared prime. Compare Step 4 to the inefficient primality test of Figure 22.1. The only difference is that we are now performing the computations modulo $X^r - 1$. The main danger in this is that even if $(X-a)^n \not\equiv_n X^n - a$, it could be that $(X-a)^n \equiv_{X^r-1,n} X^n - a$. To compensate for this, we now verify the identity for ℓ different values of a, instead of trying just one value, namely 1. The main point of the Agrawal, Kayal and Saxena paper is that this is adequate compensation.

To see this, let us assume the opposite and show that this leads to a contradiction.

Assumption: n is a composite number and the PTA algorithm declares that it is prime.

Because the number n passes all tests in Step 4, we know that

$$\text{for } a = 1, 2, \ldots, \ell,\ (X-a)^n \equiv_{X^r-1,n} X^n - a. \tag{22.1}$$

Note that in the above identity we can replace the n in $(\text{mod } X^r - 1, n)$ by any divisor of n. Let p be a prime divisor of n. [Most of our discussion is valid for any prime divisor of n. In the end we will choose a special prime divisor of n based on the conditions established in Step 2.] Then, we have

$$\text{for } a = 1, 2, \ldots, \ell,\ (X-a)^n \equiv_{X^r-1,n} X^n - a. \tag{22.2}$$

Since p is prime, we always have (see Lemma 22.1(a))

$$\text{for } a = 1, 2, \ldots, \ell,\ (X-a)^p \equiv_{X^r-1,n} X^p - a. \tag{22.3}$$

We thus see that the numbers n and p satisfy similar identities in (22.2), (22.3).

Claim 22.1 *Suppose*

$$\begin{aligned}(X-a)^{m_1} &\equiv_{X^r-1,p} X^{m_1} - a \text{ and}\\ (X-a)^{m_2} &\equiv_{X^r-1,p} X^{m_2} - a.\end{aligned}$$

Then, $(X-a)^{m_1 m_2} \equiv_{X^r-1,p} X^{m_1 m_2} - a$.

Proof:
The second assumption says that $(X-a)^{m_2} - (X^{m_2} - a) \equiv_p (X^r - 1)g(X)$, for some polynomial $g(X)$. By substituting X^{m_1} for X in this identity, we get

$$(X^{m_1} - a)^{m_2} - (X^{m_1 m_2} - a) \equiv_p (X^{m_1 r} - 1)g(X^{m_1}).$$

Since $X^r - 1$ divides $X^{m_1 r} - 1$, this shows that $(X^{m_1} - a)^{m_2} \equiv_{X^r-1,p} X^{m_1 m_2} - a$. Using this and the first assumption, we obtain

$$(X-a)^{m_1 m_2} = (X^{m_1} - a)^{m_2} \equiv_{X^r-1,p} X^{m_1 m_2} - a.$$

□

Now starting from (22.2) and (22.3), and repeatedly applying the above claim, we see that for each m of the form $p^i n^j$, $(i, j \geq 0)$, we have $(X-a)^m \equiv_{X^r-1,p} X^m - a$, for $a = 1, 2, \ldots, \ell$. (The case $i, j = 0$ corresponds to $m = 1$, and is trivially true.)

Consider the list $L = (p^i n^j : 0 \leq i, j \leq \lfloor\sqrt{r}\rfloor)$. This list has $(\sqrt{r}+1)^2 > r$ numbers. Thus, we have two numbers in the list that are congruent modulo r. Let these numbers be $m_1 = p^{i_1} n^{j_1}$ and $m_2 = p^{i_2} n^{j_2} = m_1 + kr$, where $(i_1, j_1) \neq (i_2, j_2)$. From now on we will concentrate on just these two elements of the list. Since $X^r \equiv_{X^r-1} 1$, we have $(X-a)^{m_2} = X^{m_1+kr} - a = X^{m_1} - a \equiv_{X^r-1,p} (X-a)^{m_1}$. That is,

$$\text{for } a = 1, 2, \ldots, \ell,\ \ (X-a)^{m_1} \equiv_{X^r-1,p} (X-a)^{m_2}. \tag{22.4}$$

Claim 22.2 $m_1 = m_2$.

We will prove this claim below. Let us first complete the proof of correctness by assuming this claim. From this claim and the definition of m_1 and m_2 we see that $p^{i_1} n^{j_1} = p^{i_2} n^{j_2}$. Since $(i_1, j_1) \neq (i_2, j_2)$ and p is prime, this implies that n is a power of p. That is $n = p^s$ for some s. If $s \geq 2$, Step 1 of the algorithm would already have declared that n is composite. This contradicts our assumption that the algorithm declares that n is prime. On the other hand, if $s = 1$, then n is prime, again contradicting our assumption that n is composite. We have proved that the algorithm is correct assuming Claim 22.2.

Proof of Claim 22.2: Let $h(X)$ be an irreducible factor of $(X^r-1)/(X-1)$. Then, from (22.4) we see that

$$\text{for } a=1,2,\ldots,\ell,\ (X-a)^{m_1} \equiv_{h(X),p} (X-a)^{m_2}. \tag{22.5}$$

That is, each element of the field $\mathbb{F}_p[X]/(h(X))$ of the form $X-a$ satisfies the equation $Z^{m_1}-Z^{m_2}=0$. Note that if e_1 and e_2 are two elements that satisfy this equation, then e_1e_2 also satisfies this equation. Thus, each element of the set

$$S=\left\{\prod_{a=1}^{\ell}(X-a)^{\alpha_a} : \alpha_a \in \{0,1\}\right\}$$

satisfies this equation. We will argue (based on the choice of r in Step 2) that S has 2^ℓ distinct elements. Thus, the equation $Z^{m_1}-Z^{m_2}=0$ has at least 2^ℓ roots in the field $\mathbb{F}_p[X]/(h(X))$. Note that $m_1,m_2 \leq n^{2\sqrt{r}} < 2^\ell$. That is, this polynomial has more roots than its degree. So, it must be the zero polynomial, that is $m_1=m_2$, and we are done.

We need to argue that the 2^ℓ products of the form $\prod_{a=1}^{\ell}(X-a)^{\alpha_a}$, $\alpha_a \in \{0,1\}$, give distinct elements in $\mathbb{F}_p[X]/(h(X))$. By Step 3, $p>\ell$. So, $X-a$, for $a=1,2,\ldots,\ell$, are distinct irreducible elements of $\mathbb{F}_p[X]$. Since elements of $\mathbb{F}_p[X]$ factorize uniquely into irreducible factors, the 2^ℓ products, $\prod_{a=1}^{\ell}(X-a)^{\alpha_a}$, $\alpha_a \in \{0,1\}$, are distinct elements of $\mathbb{F}_p[X]$. But are they distinct in $\mathbb{F}_p[X]/(h(X))$? Each such product is a distinct element of $\mathbb{F}_p[X]$ of degree at most ℓ, so the difference of any two is a non-zero polynomial of degree at most ℓ. If we can somehow ensure that the degree of $h(X)$ is at least $\ell+1$, then these products will be distinct in $\mathbb{F}_p[X]/(h(X))$.

How do we ensure that $h(X)$ has degree at least $\ell+1$? Recall that the number p in the argument so far is an arbitrary prime divisor of n. It is time to choose p. By Step 2, we know that the order of n modulo r is divisible by a prime $q \geq \ell+1$. Since q is prime there must be a prime factor p of n whose order w modulo r is divisible by q. In particular, $w \geq q \geq \ell+1$. Fix one such p.

Claim 22.3 *w divides $\deg(h)$, so $\deg(h) \geq w \geq \ell+1$. (Actually, $\deg(h)=w$, but we won't need this.)*

Proof:
Let η be a root of $h(X)$ in a suitable extension of $\mathbb{F}_p$. Since $h(X)$ divides X^r-1, we have $\eta^r=1$. Since $\eta \neq 1$ (h is irreducible) and r is prime, the order of η in this field is r. Since r does not divide p (because r does not divide n in Step 2), $\eta,\eta^p,\eta^{p^2},\ldots,\eta^{p^{w-1}}$, are distinct elements of the field. Since, $h(X)^p=h(X^p)$, and $h(\eta)=0$, we have $h(\eta^{p^i})=0$ for $i=0,1,\ldots,w-1$. So $h(X)$ has at least w distinct roots in a field. Thus, $h(X)$ must have degree at least w.
We have $X^r=1$ in $\mathbb{F}_p[X]/(h(X))$, because $h(X)$ divides X^r-1. In the implementation of Step 2, we ensure that r does not divide n; in particular, $r \neq p$. So, 1 is not a root of $(X^r-1)/(X-1)$ in $\mathbb{F}_p$, and $h(X) \neq X-1$. Since r is prime, and $X \neq 1$, the order of X in $\mathbb{F}_p[X]/(h(X))$ is exactly r. But the order of an element must divide the order, $p^{\deg(h)}-1$, of the multiplicative group of the field. That is, r divides $p^{\deg(h)}-1$, implying that w divides $\deg(h)$. This completes the proof of Claim 22.3 and Claim 22.2. □
The above claims immmediately lead to the central theorem of this lecture.

Theorem 22.1 *The procedure PTA declares that a number p is prime only if p is prime.*

[This lecture was delivered by Prof. Jaikumar from Tata Institute of Fundamental Research, Mumbai.]

Part II

Examples

Chapter 23

Akshat Verma

23.1 Example 1

Example 23.1 *Show that the prime divisors of* $2^p - 1$*, where* p *is any odd prime are of the form* $2kp + 1$*.*

In order to prove the above, we first prove a general result.

Theorem 23.1 *If* p *and* q *are odd primes and* $q|a^p - 1$*, then either* $q|a - 1$ *or* $q = 2kp + 1$ *for some integer* k*.*

Proof: Since $q|a^p - 1$, we have

$$a^p =_q 1 \tag{23.1}$$

Also, by FLT, we have

$$a^{q-1} =_q 1 \tag{23.2}$$

We also know that if order of a modulo q should be a factor of all r such that $a^r =_q 1$. Hence, the order of a modulo q should be either p or 1, as p is prime. If the order of a modulo q is 1, we have $q|a - 1$.Otherwise, By the earlier argument, $q - 1$ should also be a multiple of p, i.e.,

$$q - 1 = kp \tag{23.3}$$

Hence, $q = kp + 1$. Also, since we have the fact that q is odd, we get $q = 2kp + 1$. $\square$ We now make the note that $a - 1$ for $a = 2$ is 1 and hence, the first case of Theorem 1 is not possible. Hence, all odd prime divisors of $2^p - 1$ have the form $2kp + 1$. We also note that there are no even divisors of $2^p - 1$ as it is an odd number. This completes the required proof.

23.2 Example 2

Example 23.2 *Assume that* p *and* q *are distinct odd primes such that* $p - 1|q - 1$*. If* $gcd(a, pq) = 1$*, show that* $a^{q-1} =_{pq} 1$*.*

Since a and pq has no common factors and p and q are prime, we know that $gcd(a, p) = gcd(a, q) = 1$. Hence, we know the following from FLT:

$$a^{p-1} =_p 1 \tag{23.4}$$

$$a^{q-1} =_q 1 \tag{23.5}$$

By the assumption that $p-1|q-1$, we have

$$q-1 = k(p-1) \quad \text{for some } k \geq 1 \tag{23.6}$$

Hence, we have

$$a^{q-1} = a^{k(p-1)} = a^{(p-1)^k} =_p 1^k = 1 \tag{23.7}$$

i.e., $a^{q-1} =_p 1$. or

$$p|a^{q-1} - 1 \tag{23.8}$$

. Also, by Eqn. 23.5 we have

$$q|a^{q-1} - 1 \tag{23.9}$$

By Eqn. 23.9 and 23.8 and the fact that p and q are primes, we have

$$pq|a^{q-1} - 1 \tag{23.10}$$

This proves the required statement.

23.3 Example 3

Theorem 23.2 *Show the more general result of the mulitplicativity of Euler's function, i.e, show that*

$$\phi(ab) = \frac{d\phi(a)\phi(b)}{\phi(d)} \tag{23.11}$$

where $d = gcd(a, b)$.

Proof: Let us express d as a product of its prime factors p_i, i.e.,

$$d = p_1^{\alpha_1}...p_k^{\alpha_k}$$

Similarly, we can write a and b as

$$a = p_1^{\alpha_1}...p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}}...p_{k+m}^{\alpha_{k+m}} \tag{23.12}$$

$$b = p_1^{\alpha_1}...p_k^{\alpha_k} p_{k+1'}^{\alpha'_{k+1}}...p_{(k+n)'}^{\alpha'_{k+n}} \tag{23.13}$$

Now, we use the following theorem

$$\phi(m) = m\Pi_{p|m}(1 - \frac{1}{p}) \tag{23.14}$$

where the product is over all the distinct prime roots p of m.

It is easy to see now that

$$\phi(ab) = ab((1-\frac{1}{p_1})...(1-\frac{1}{p_m}))((1-\frac{1}{p_{k+1'}})...(1-\frac{1}{p_{k+n'}})) \tag{23.15}$$

$$= a((1-\frac{1}{p_1})...(1-\frac{1}{p_m}))b((1-\frac{1}{p_{k+1'}})...(1-\frac{1}{p_{k+n'}})) \tag{23.16}$$

$$= \phi(a)\frac{\phi(b)}{(1-\frac{1}{p_1})...(1-\frac{1}{p_k})} \tag{23.17}$$

$$= \frac{\phi(a)\phi(b)}{\frac{\phi(d)}{d}} \tag{23.18}$$

$$= \frac{\phi(a)\phi(b)d}{\phi(d)} \tag{23.19}$$

□

23.4 Example 4

Theorem 23.3 *For $n \geq 2$,*

$$u_{2n-1} = u_n^2 + u_{n-1}^2 \quad (23.20)$$
$$u_{2n} = u_{n+1}^2 - u_{n-1}^2 \quad (23.21)$$

Proof: The proof is by induction.
Base Case: $n = 2$

$$u_3 = 2 = 1 + 1 = u_2^2 + u_1^2 \quad (23.22)$$
$$u_4 = 3 = 4 - 1 = u_3^2 - u_1^2 \quad (23.23)$$

Induction Hypothesis:
Let us assume that the theorem holds for $n = k$; then we have

$$u_{2k-1} = u_k^2 + u_{k-1}^2 \quad (23.24)$$
$$u_{2k} = u_{k+1}^2 - u_{k-1}^2 \quad (23.25)$$

Induction Step:
Adding the two equations we get:

$$u_{2k+1} = u_{k+1}^2 + u_k^2 \quad (23.26)$$

This completes the proof for the odd case. Also, we have

$$u_{2k+2} = u_{2k+1} + u_{2k} \quad (23.27)$$
$$= u_{k+1}^2 + u_k^2 + u_{k+1}^2 - u_{k-1}^2 \quad (23.28)$$
$$= u_{k+1}^2 + u_k^2 + u_k^2 + u_{k-1}^2 + 2u_k u_{k-1} - u_{k-1}^2 \quad (23.29)$$
$$= u_{k+1}^2 + u_k^2 + u_k^2 + 2u_k(u_{k+1} - u_k) \quad (23.30)$$
$$= u_{k+1}^2 + u_k^2 + 2u_k u_{k+1} - u_k^2 \quad (23.31)$$
$$= (u_{k+1} + u_k)^2 - u_k^2 \quad (23.32)$$
$$= u_{k+2}^2 - u_k^2 \quad (23.33)$$

□

23.5 Example 5

Theorem 23.4 *If p' is a prime such that $p' \equiv_4 1$ and if $p = 2p' + 1$ is also a prime, then 2 is a primitve root (mod p).*

Proof: By Fermat's Little Theorem, we have

$$2^{p-1} \equiv_p 1 \quad (23.34)$$

So, to prove that 2 is a primitve root $modp$, we only need to show that there does not exist a $k < p - 1$, s.t.

$$2^k \equiv_p 1 \quad (23.35)$$

To show this, we assume that there does exist such a k and without loss of generality we take the smallest such k. Hence, k is the order of a modulo p. Because of Eqns. 23.34 and 23.35, we have $k|(p-1)$. Also, we have

$p = 2p' + 1$. Hence, we have $k | 2p'$, which means that either $k = 2$ or $k = p'$. It is obvious that $k \neq 2$ as $2^2 \equiv_p 4$. Hence, the only possible case is $k = p'$, i.e.,

$$2^{p'} \equiv_p 1 \quad (23.36)$$

$$2^{(p-1)/2} \equiv_p 1 \quad (23.37)$$

Also, $p' = 4n + 1$ and $p = 2p' + 1$ leads to $p \equiv_8 3$. Hence, $\left\lfloor \begin{matrix} 2 \\ p \end{matrix} \right\rfloor = -1$, i.e. , there does not exist any such k and $p - 1$ is the order of 2 (mod p), i.e., 2 is a primitive root of p. □

Chapter 24

Rahul Gupta

24.1 Linear Congruences

Exercise 24.1 *If p is an odd prime, then prove that there are infinite primes of the form $2kp+1$. You may use the result that if b is prime, then $x^a \equiv_b 1 \Rightarrow a|(b-1) \vee x \equiv_b 1$.*

Solution: Note that the result is immediate from Dirichlet's theorem. Here we present an alternate proof. We shall prove the result by contradiction. Assume that there are only r primes of the form $2kp+1$. Let $p_1, \dots, p_r$ those r primes. Define s and t as

$$s = 2p_1p_2 \dots p_r \quad (24.1)$$

$$t = s^{p-1} + s^{p-2} + \dots + 1 \quad (24.2)$$

$$= \frac{(s^p - 1)}{s-1} \quad (24.3)$$

Note that since $p_i = 2k_ip + 1$, we have $p_i \equiv_p 1$. Hence $s \equiv_p 2$. Now consider a prime divisor q of t. Hence,

$$s^p \equiv_q 1 \quad (24.4)$$

Therefore, either $s \equiv_q 1$ or $p|(q-1)$.

1. Consider the case $s \equiv_q 1$. If $s \equiv_q 1$, then $s^i \equiv_q 1$ for all i. Hence,

   $$t \equiv_q p \quad (24.5)$$

   But since q divides t, therefore, $t \equiv_q 0$. So it must be that $p = q$. But if $p = q$, then $s \equiv_q 1 \equiv_p 1$, which contradicts $s \equiv_p 2$. So, this case is impossible.

2. Consider the case $p|(q-1)$. Therefore, $q = 2kp+1$, since $(q-1)$ is even and a multiple of p. So q must one of the p_i's. So $q|s$ and consequently $q|s^i$ for $1 \le i \le p-1$. Therefore $t \equiv_q 1$ which violates $t \equiv_q 0$.

So, there are an number of infinite primes of the form $2kp+1$ where p is an odd prime. □

24.2 Euler Function

Exercise 24.2 *Define $S(m) = \{a \mid \phi(a) = m, a > 0\}$. Prove that*

1. *$S(m)$ is finite for all m.*
2. *$S(m) = \phi$ whenever m is an odd integer greater than 1.*

Solution: Let the unique prime factorization of any integer a in $S(m)$ be given by:

$$a = {p_1}^{k_1}{p_2}^{k_2}\dots{p_r}^{k_r} \tag{24.6}$$

Therefore,

$$\phi(a) = \prod_{i=1}^{i=r}(p_i^{k_i} - p_i^{k_i-1}) \tag{24.7}$$

$$= \prod_{i=1}^{i=r} p_i^{k_i-1}(p_i - 1) \tag{24.8}$$

If $\phi(a) = m$, then surely $(p_i - 1)|m$ for all $1 \le i \le r$. Since there are only finite number of divisors of m, then our possible choices for p_i are restricted. If m has d_m different divisors, then we can choose a maximum of d_m different primes. Further, since $(p_i - 1)|m$, we have

$$p_i^{k_i-1} \le m,\ 1 \le i \le r. \tag{24.9}$$

$$\text{or } k_i \le 1 + \frac{log(m)}{log(p_i)} \tag{24.10}$$

$$\le 1 + \frac{log(m)}{log(2)} \tag{24.11}$$

Hence, we have a finite upper bound on the possible prime factors and also their exponents. Therefore, the number of a's such that $\phi(a) = m$, is finite. Infact,

$$|S(m)| \le d_m(1 + \frac{log(m)}{log(2)}) \tag{24.12}$$

Further, $p_i^{k_i-1}(p_i - 1)$ is even for all primes p_i except when $p_i = 2$ and $k_i = 1$. Hence, for all odd $m > 1$, $S(m) = \phi$. □

24.3 Primitive Roots

Exercise 24.3 *Prove that if $n > 2$, then the product of all primitive roots of n is congruent to 1 modulo n.*

Solution: Let a be any one of the primitive roots of n. Now, all the primitive roots of n lie in the set

$$R = \{a^i \mid gcd(a^i, n) = 1\} \tag{24.13}$$

Let $\{a^{i_1}, a^{i_2}, \dots, a^{i_m}\}$ be all the primitive roots of n, where $m = \phi(\phi(n))$. Therefore, the required product is given by

$$\pi = a^{i_1+i_2+\dots+i_m} \tag{24.14}$$

Claim 24.1 *The sum of all numbers coprime to an even integer b is divisible by $\phi(b)$.*

Proof: Let $S = \sum_{j \perp b} j$. If j is coprime, then so is $b - j$. Therefore,

$$S = \sum_{j \perp b}(b - j) \tag{24.15}$$

$$= b\phi(b) - S. \tag{24.16}$$

So, $S = \frac{1}{2}b\phi(b)$. And hence $\phi(b)|b$ whenever b is even. $\square$

Now, $\phi(n)$ is always even since $n > 2$. Therefore the claim applies, and all the $\phi(\phi(n))$ integers that are coprime to $\phi(n)$ add up to be a multiple of $\phi(n)$, say $k\phi(n)$. Hence,

$$\pi = a^{k\phi(n)} \tag{24.17}$$
$$\equiv_n 1 \quad \text{(because } a \perp n) \tag{24.18}$$

$\square$

24.4 Quadratic Reciprocity

Exercise 24.4 *Prove that if p and q are two distinct primes that differ by 4, then atleast one of the equations $x^2 \equiv_{pq} 5$, $x^2 \equiv_{pq} 10$ has no solutions.*

Solution: We shall prove the result by contradiction. Assume that both the given equations have atleast one solution each. Hence 5 and 10 are quadratic residues modulo pq. Therefore they are also quadratic residues modulo p and q.

$$\left\lfloor \begin{matrix} 5 \\ pq \end{matrix} \right\rfloor = 1 \tag{24.19}$$
$$\left\lfloor \begin{matrix} 10 \\ pq \end{matrix} \right\rfloor = 1 \tag{24.20}$$
$$\Rightarrow \left\lfloor \begin{matrix} 5 \\ p \end{matrix} \right\rfloor = 1 \quad \text{and} \quad \left\lfloor \begin{matrix} 10 \\ p \end{matrix} \right\rfloor = 1 \tag{24.21}$$
$$\Rightarrow \left\lfloor \begin{matrix} 5 \\ q \end{matrix} \right\rfloor = 1 \quad \text{and} \quad \left\lfloor \begin{matrix} 10 \\ q \end{matrix} \right\rfloor = 1 \tag{24.22}$$

Note that the case $p = 5$ and $q = 2$ doesn't arise because p and q differ by exactly 4. Now since the Legendre symbol is multiplicative, we get

$$\left\lfloor \begin{matrix} 2 \\ p \end{matrix} \right\rfloor = \left\lfloor \begin{matrix} 10 \\ p \end{matrix} \right\rfloor \Big/ \left\lfloor \begin{matrix} 5 \\ p \end{matrix} \right\rfloor = 1 \text{ and } \left\lfloor \begin{matrix} 2 \\ q \end{matrix} \right\rfloor = \left\lfloor \begin{matrix} 10 \\ q \end{matrix} \right\rfloor \Big/ \left\lfloor \begin{matrix} 5 \\ q \end{matrix} \right\rfloor = 1 \tag{24.23}$$

Now, $\left\lfloor \begin{matrix} 2 \\ p \end{matrix} \right\rfloor = 1 \Leftrightarrow p \equiv_8 \pm 1$. Hence both p and q are of the form ± 1 mod 8. The various possibilites for $p - q$ (mod 8) are 0,2,6. Since $p - q \equiv_8 4$, we arrive at a contradiction. So, atleast one of the given congruences has no solution. $\square$

24.5 Quadratic Residues

Exercise 24.5 *Assuming p to be an odd prime, prove the following :*

1. *Product of all quadratic residues of p is $\equiv_p\ (-1)^{(p+1)/2}$.*
2. *If $p \equiv_4 1$ then the sum of all quadratic residues of p equals $\frac{1}{4}p(p-1)$.*

Solution: (1) Let r be any primitive root of p. The set of quadratic residues of p is exactly equal to the set

$\{r^{2k} \mid 2 \leq 2k \leq p-1\}$. Hence the product of the quadratic residues is given by

$$\pi = \prod_{k=1}^{(p-1)/2} r^{2k} \quad (24.24)$$

$$= r^{\sum_{k=1}^{(p-1)/2} 2k} \quad (24.25)$$

$$= r^{(p-1)(p+1)/4} \quad (24.26)$$

$$= (r^{(p-1)/2})^{(p+1)/2} \quad (24.27)$$

Now since r is a primitive root, therefore, $r^{(p-1)/2} \equiv_p -1$. This is so because the only other choice for $r^{(p-1)/2}$ is 1, which is impossible because $order_p(r) = p-1$. Hence,

$$\pi \equiv_p (-1)^{(p+1)/2} \quad (24.28)$$

□ *Solution:* (2) Let $p = 4k+1$. Take any arbitrary integer $x \in [1, p-1]$. Let $y = p - x$. y is the mirror image of x about the point $(p-1)/2$ on the real axis. We have,

$$x \equiv_p -y \quad (24.29)$$

$$\Rightarrow x^{(p-1)/2} \equiv_p (-1)^{(p-1)/2} y^{(p-1)/2} \quad (24.30)$$

$$\Rightarrow x^{(p-1)/2} \equiv_p y^{(p-1)/2}, \text{ since } (p-1)/2 \text{ is even.} \quad (24.31)$$

Therefore, x is a quadratic residue $\Leftrightarrow$ y is a quadratic residue. Hence, we can conclude the following

- The residues are split equally before and after $(p-1)/2(=2k)$ (Strictly speaking, $2k$ is a part of the first half). Moreover, since p is a prime, there are exactly $(p-1)/2(=2k)$ quadratic residues. Out of these, exactly k lie in $[1, 2k]$.
- The sum of a quadratic residue $x \in [1, 2k]$ and its 'mirror' residue $p - x$ is p, which is independent of x.

Hence the total sum of all residues is given by $\sum_{x \ is \ a \ q.r \ in \ [1,2k]} x + p - x \ = \ kp \ = \ \frac{1}{4}(p-1)p$. □

Chapter 25

Gaurav Gupta

25.1 Fibonacci Numbers

Exercise 25.1 *Prove that, for any number m, there must be a Fibonacci number F_k such that $F_k \equiv_m 0$, and further that, $k \leq m^2$*

Solution: Begin by considering the set A,

$$(a_i, i = 1, 2, 3, ..|a_n \equiv_m F_n)$$

Since the terms of that sequence are remainders left on division by m, they are numbers between 0 and $m - 1$, of which there are m. Further, there are only m^2 ordered pairs of remainders possible. (There are m choices for the first number in the ordered pair, and for each choice, m choices for the second number.) We now make two observations:

1. Because of the addition rule for congruences, the a_i sequence satisfies $a_{n+2} \equiv_m a_{n+1} + a_n$. This means that once we know two terms of the sequence, all the rest are determined.
2. $F_0 \equiv_m 0$ and $F_1 \equiv_m 1$. Thus, the ordered pair of remainder (0,1) occurs.

Since there are $m^2 + 1$ remainders arising from the Fibonacci numbers F_0 through F_{m^2}, but only m^2 different ordered pairs of remainders, implying m^2 different remainders (By 1^{st} Observation), the remainders must repeat (By Pigeonhole principle). Further, since they are uniquely defined forwards and backwards, and since 0 occurs at F_0, 0 must reoccur. Hence, there are Fibonacci numbers divisible by m, regardless of what m is. □

25.2 Fermat's Little theorem

Exercise 25.2 *Show that, every possible divisor of the number $F_n = 2^{2^n} + 1$, $n \geq 5$, has the form*

$$p = h.2^{n+2} + 1$$

with an integer h.

Solution: If $p \mid F_n = 2^{2^n} + 1$, then

$$\begin{aligned} & 2^{2^n} && \equiv_p -1 \mod p \\ \Longrightarrow\ & 2^{2^n+1} && \equiv_p 1 \\ \Longrightarrow\ & 2^{2^n+2} && \equiv_p 1 \qquad \text{since } a \equiv_n b \Longrightarrow a^k \equiv_n b^k \\ \Longrightarrow\ & 2^{2^n+2} - 1 && \equiv_p 0 \end{aligned}$$

Now, we make use of Fermat's little theorem which is as follows:

Theorem 25.1 *If p is a prime number and a is a natural number, then*

$$a^p \equiv_p a$$

Furthermore, if p does not divide a, then there exists some smallest exponent d such that

$$a^d - 1 \equiv_p 0$$

and d divides $p - 1$.

Getting back to our problem, we conclude that we have

$$\begin{aligned} & 2^{n+2} \mid (p-1) \\ \Longrightarrow\ & p = h.2^{n+2} + 1 \end{aligned}$$

□

25.3 Chinese Remainder Theorem

Exercise 25.3 *Prove that, $x^2 \equiv_n x$ has exactly 2^k different solutions, where k is the number of distinct primes of n.*

Solution: Let $n = m_1 m_2 ... m_k$, where $m_i, 1 \le i \le k$ are powers of distinct primes. We know:

$$x^2 \equiv_n x \Longrightarrow x(x-1) \equiv_n 0$$

Note that, m_i are relatively prime, we have:

$$\{x \mid x(x-1) \equiv_n 0\} \iff \{x \mid x(x-1) \equiv_{m_i} 0, \forall 1 \le i \le k\}$$

So, the number of solutions should be the same for both sets. Also note:

$$gcd(x, x-1) = 1$$

So the solution of $x(x-1) \equiv_{m_i} 0$ must satisfy:

$$x \equiv_{m_i} 0 \bigvee x \equiv_{m_i} 1, \forall 1 \le i \le k$$

So we can get 2^k different systems. By the Chinese Remainder theorem, each system must have one unique solution modulo $n = m_1 m_2 ... m_k$. Furthermore, we can also show that these systems have distinct solutions. If two different systems have the same solution x, then within these two systems must exist the following two different equations associated with some m_i:

$$x \equiv_{m_i} 0$$

$$x \equiv_{m_i} 1$$

But this is impossible.
So we can conclude that the equation $x^2 \equiv_n x$ has exactly 2^k different solutions. □

25.4 Euler's Criterion

Exercise 25.4 *Give solutions for :*

$$x^2 \equiv_{79} 5$$

Solution: Note that 79 is an odd prime, and gcd(5,79)=1, ie 79 does not divide 5. So our problem can be generalized to solving

$$x^2 \equiv_p a$$

where p is odd and $gcd(a,p) = 1$.

$$\Longrightarrow a^{\frac{(p-1)}{2}} \equiv_p 1 \text{ by Euler's criterion}$$

Now, for $x = \pm a^{\frac{p+1}{4}}$ we have

$$x^2 \equiv_p a^{\frac{p+1}{2}} \equiv_p aa^{\frac{p-1}{2}} \equiv_p a$$

Thus the solution of $x^2 \equiv_p a$ are $x \equiv_p \pm a^{\frac{p+1}{4}}$. (We know that there are exactly two solutions mod p)
Applying this to $x^2 \equiv_{79} 5$: we have $p = 79$ and $\frac{(p+1)}{4} = 20$, so the solutions are $x \equiv_{79} \pm 5^{20}$.
Now, $5^{20} \equiv_{79} 20$. Hence the solutions are $x \equiv_{79} \pm 20$. □

25.5 GCD

Exercise 25.5 *If $gcd(b,c) = 1$, prove that*

$$gcd(a,bc) = gcd(a,b)gcd(a,c)$$

Solution: Suppose $gcd(b,c) = 1$. Let

$$\begin{aligned} e &= gcd(a,bc) \\ f &= gcd(a,b) \\ g &= gcd(a,c) \end{aligned}$$

$$\begin{array}{lll} f \mid b \text{ and } g \mid c & \Longrightarrow gcd(f,g) = 1 & (0) \\ f \mid a \text{ and } g \mid a & \Longrightarrow fg \mid a & (1) \\ f \mid b \text{ and } g \mid c & \Longrightarrow fg \mid bc & (2) \\ (1) \text{ and } (2) & \Longrightarrow fg \mid gcd(a,bc) = e & (3) \end{array}$$

Next, $f = ax + by$, $g = aX + cY$

$$\begin{aligned} fg &= (ax+by)(aX+cY) \\ &= a^2xX + acxY + bayX + bcyY \quad (4) \end{aligned}$$

But, $e \mid a, e \mid bc \Longrightarrow e \mid RHS(4) \Longrightarrow e \mid fg$ ... (5)
From (3) and (5), we obtain that $e = fg$. □

Chapter 26

Ashish Rastogi

26.1 Greatest Common Divisor

Exercise 26.1 *A polynomial f with integer coefficients is called* primitive *if*

$$f(x) = a_0 + a_1 x + \ldots a_n x^n \qquad \textit{and} \qquad (a_0, a_1, \ldots, a_n) = 1.$$

Prove that the product of two primitive polynomials is primitive.

Answer Suppose f and g are two primitive polynomials. That is

$$f(x) = \sum_{i=0}^{n_1} a_i x^i \qquad \text{and} \qquad g(x) = \sum_{i=0}^{n_2} b_i x^i$$

where $(a_0, a_1, \ldots, a_n) = (b_0, b_1, \ldots, b_n) = 1$. The product of two primitive polynomials $h(x) = f(x) \cdot g(x)$. We have

$$h(x) = \sum_{i=0}^{n_1+n_2} c_i x^i \qquad \text{where } c_i = \sum_{t=0}^{i} a_t b_{i-t}$$

We need to show that $(c_1, c_2, \ldots, c_{n_1+n_2}) = 1$ given that $(a_1, a_2, \ldots, a_{n_1}) = 1$ and $(b_1, b_2, \ldots, b_{n_2}) = 1$. The fact that $(a_1, a_2, \ldots, a_{n_1}) = 1$ implies that there does not exist a prime p such that $p \mid a_i$ for all $1 \le i \le n_1$. Similarly, there does not exist a prime p such that $p \mid b_i$ for all $1 \le i \le n_2$.

Claim 26.1 *The prime p divides c_k for all $k < i + j$.*

Proof: We have

$$c_k = \sum_{t=0}^{k} a_t b_{k-t}$$

We claim that in any term $a_t b_{k-t}$ of the above summation, either $t < i$ or $k - t < j$. In order to observe this, assume that in some term of the summation, we have both $t \ge i$ and $k - t \ge j$. Then summing these two inequalities we get $t + (k - t) \ge i + j$ $(\Rightarrow)$ $k \ge i + j$, but since $k < i + j$, we arrive at a contradiction.

Since in any term $a_t b_{k-t}$ for $0 \le t \le k$, we have either $t < i$ or $k - t < j$, it follows that either $a_t \in \{a_0, a_1, \ldots, a_{i-1}\}$ or $b_{k-t} \in \{b_0, b_1, \ldots, b_{j-1}\}$. Therefore we have either $p \mid a_t$ (if $a_t \in \{a_0, a_1, \ldots, a_{i-1}\}$) or $p \mid b_{k-t}$ (if $b_t \in \{b_0, b_1, \ldots, b_{j-1}\}$). In both cases, we have $p \mid a_t b_{k-t}$. Therefore since $p \mid a_t b_{k-t}$ for all $0 \le t \le k$, it follows that $p \mid \sum_{t=0}^{k} a_t b_{k-t}$ $(\Rightarrow)$ $p \mid c_k$. □

Claim 26.2 *The prime p does not divide c_{i+j}.*

Proof: We have

$$c_{i+j} = \sum_{t=0}^{i+j} a_t b_{i+j-t}$$

We will that p divides all terms in the expansion of c_{i+j} except $a_i b_j$. First of all, note that since $p \nmid a_i$ and $p \nmid b_j$ and since p is prime, $p \nmid a_i b_j$. Now consider any term $a_t b_{i+j-t}$ with $t \neq i$. Once again, for any term of the expansion of c_{i+j}, we claim that either $t < i$ or $i + j - t < j$. For the sake of contradiction, assume that $t > i$ and $i + j - t > j$. Further, since $t \neq i$, we have $t > i + 1$. Adding the two inequalities, we get $i + j > i + j + 1$, which brings us to a contradiction. Therefore, for any term $a_t b_{i+j-t}$ with $t \neq i$, we have either $p \mid a_t$ or $p \mid b_{i+j-t}$. It follows that $p \mid \sum_{t=0,t\neq i}^{i} +j a_t b_{i+j-t}$. But since $p \nmid a_i b_j$, we have $p \nmid c_{i+j}$. □

Therefore, for any prime p, we have shown that there exists an integer m ($0 \leq m \leq n_1 + n_2$) such that $p|c_l$ for $1 \leq l < m$ and $p \nmid c_m$. Therefore, there is no prime p such that $p \mid c_l$ for $0 \leq l \leq n_1 + n_2$. It follows that $(c_0, c_1, \ldots, c_{n_1+n_2}) = 1$, which completes the proof.

26.2 General Number Theory

Exercise 26.2 *Prove that S_n defined as*

$$S_n = \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{i} + \ldots + \frac{1}{n}$$

is not an integer for all positive integers $n \geq 2$.

Answer We present a proof by contradiction. Let us assume that S_n is an integer for some integer n. Let k be an integer such that $2^k \leq n < 2^{k+1}$. Note that since $n \geq 2$, $k \geq 1$.

Claim 26.3 *The minimum integer m such that for all $2 \leq i \leq n$, $i \mid m$ is*

$$m = 2^k \cdot 3 \cdot 5 \cdot 7 \cdot 9 \cdot \ldots$$

Proof: Any integer i such that $2 \leq i \leq n$, we have $i = 2^j \cdot (2l + 1)$, where $2l + 1 < m$ and $j \leq k$. Therefore $2^j \mid m$ and $2l + 1 \mid m$. Therefore $2^j \cdot (2l + 1) \mid m$. Hence, we have $i \mid m$ for all $2 \leq i \leq n$. □

Consider the number $S_n \cdot m$,

$$S_n \cdot m = \frac{m}{2} + \frac{m}{3} + \ldots + \frac{m}{i} + \ldots + \frac{m}{n}$$

Note that since $k \geq 1$, m must be even. Assuming that S_n is an integer, $S_n \cdot m$ is also even (product of an integer with an even number is also even). We will show that $\sum_{i=2}^{n} \frac{m}{i}$ is an odd integer, which is impossible since $S_n \cdot m = \sum_{i=2}^{n} \frac{m}{i}$, thus arriving at a contradiction.

Firstly, note that $\frac{m}{i}$ is an integer for each $i \leq 2 \leq n$ since $i \mid m$ (from the claim). Further, for each $i \leq 2 \leq n$, except for $i = 2^k$, we have $i = 2^j \cdot (2l + 1)$ where $j < k$. Therefore we have

$$\frac{m}{i} = \frac{2^k \cdot 3 \cdot 5 \cdot 7 \cdot 9 \cdot \ldots}{2^j \cdot (2l + 1)} = 2^{k-j} \cdot (\textit{product of odd numbers})$$

Since $j < k$, $k - j \geq 1$ and therefore $2^{k-j} \cdot (\textit{product of odd numbers})$ is an even number. Therefore,

$$\sum_{i=2..n}^{i \neq 2^k} \frac{m}{i} = \textit{an even integer}$$

For $i = 2^k$, $\frac{m}{i} = \frac{m}{2^k} = 3 \cdot 5 \cdot 7 \cdot 9 \cdot \ldots$ which is a product of odd numbers, and hence must be odd.

$$\sum_{i=2..n}^{i \neq 2^k} \frac{m}{i} + \frac{m}{2^k} = \textit{an even integer} + \textit{an odd integer} = \textit{an odd integer}$$

And therefore

$$\sum_{i=2}^{n} \frac{m}{i} = \textit{an odd integer}$$

We have shown that $S_n \cdot m$ is even and $\sum_{i=2}^{n} \frac{m}{i}$ is odd, but since $S_n \cdot m = \sum_{i=2}^{n} \frac{m}{i}$, this is impossible. Hence our assumption that S_n is an integer fails and we arrive at a contradiction.

26.3 Fibonacci Numbers

Exercise 26.3 *Let F_n be the nth term in the Fibonacci sequence. Show that a prime $p > 5$ divides either F_{p-1} or F_{p+1}.*

Answer Consider the nth Fibonacci number F_n. Let α and β be the two roots of $x^2 - x - 1$, such that $\alpha = \frac{1+\sqrt{5}}{2}$. We have:

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$$

Plugging in $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$, we get

$$F_n = \frac{(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n}{\sqrt{5}}$$

$$= \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$$

$$= \sum_{i=0}^{n} \{ \binom{n}{i} (\sqrt{5})^i 1^{n-i} - \binom{n}{i} (-\sqrt{5})^i 1^{n-i} \} / (2^n \sqrt{5})$$

which recuces to

$$= \sum_{i=1}^{odd\ i \leq n} \frac{\binom{n}{i} 5^{i/2} 2}{2^n \sqrt{5}}$$

$$= \sum_{i=1}^{odd\ i \leq n} (\binom{n}{i} 5^{(i-1)/2}) / (2^{n-1})$$

Therefore

$$F_n 2^{n-1} = \binom{n}{1} + \binom{n}{3} 5 + \binom{n}{5} 5^2 + \ldots \tag{26.1}$$

If n is some prime number $p > 5$, then we have

$$F_p 2^{p-1} = \binom{p}{1} + \binom{p}{3} 5 + \binom{p}{5} 5^2 + \ldots + 5^{(p-1)/2}$$

Note that $2^{p-1} \equiv_p 1$ (from Fermat's Little Theorem). Further, since p is a prime $\begin{pmatrix} p \\ i \end{pmatrix} \equiv_p 0$ for all $1 \le i < p$. Taking modulo p on both sides, the above equation reduces to

$$F_p \equiv_p 5^{(p-1)/2}$$

From Euler's criterion, we know that if p is an odd prime and $(a, p) = 1$, then $a^{(p-1)/2} \equiv_p \pm 1$. Therefore, plugging $a = 5$ in this equation, we have

$$F_p \equiv_p \pm 1$$

Recall from the lectures that $F_n^2 = F_{n+1}F_{n-1} + (-1)^{n-1}$. If n is an odd prime then $n - 1$ is even and hence the identity reduces to

$$F_p^2 = F_{p+1}F_{p-1} + 1$$

Since $F_p \equiv_p \pm 1$, we have $F_p^2 \equiv_p 1$, and therefore

$$F_{p+1}F_{p-1} \equiv_p 0$$

Since p is a prime, therefore either $p \mid F_{p+1}$ or $p \mid F_{p-1}$, which completes the proof.

26.4 Quadratic Residues

Exercise 26.4 *Let p be a prime. The Diophantine equation*

$$x^2 + y^2 = p$$

is soluble in integers x and y if and only if $p = 2$ or $p \equiv_4 1$.

Answer Note that $2 = 1^2 + 1^2$ and therefore $x^2 + y^2 = 2$ has a solution in integers. Next, we consider primes $p > 2$.

$\Rightarrow$ First we show that if x and y are integer solutions to the equation $x^2 + y^2 = p$, then $p \equiv_4 1$. Note that since p is an odd prime, both x and y cannot be even or odd at the same time. Without loss of generality, assume that x is even and y is odd. We have $x^2 \equiv_4 0$ (since x is even) and $y^2 \equiv_4 1$ (since y is odd). Therefore $x^2 + y^2 \equiv_4 1$, which completes one side of the proof.

($\Leftarrow$) Now, we show that if $p \equiv_4 1$ then $x^2 + y^2 = p$ is soluble in integers. We will first show that there exists an integer x_0 such that $0 < x_0 < p/2$ where $x^2 + 1 \equiv_p 0$. Rewriting this equation, we need to show that that $x^2 \equiv_p -1 \;\Rightarrow\; x^2 \equiv_p p - 1$. Therefore, we need to show that $p - 1$ is a quadratic residue modulo p.

Recall that a is a quadratic residue modulo a prime p if $p \nmid a$ and $x^2 \equiv_p a$ is soluble. By Euler's criteria, we know that a is a quadratic residue modulo p if and only if

$$a^{(p-1)/2} \equiv_p 1$$

Consider $(p-1)^{(p-1)/2}$,

$$\begin{array}{rll} & (p-1)^{(p-1)/2} & \\ \equiv_p & (-1)^{(p-1)/2} & \text{since } -1 \equiv_p (p-1) \\ = & (-1)^{((4v+1)-1)/2} & \text{since } p \equiv_4 = 1 \text{, so } p = 4v+1 \\ = & (-1)^{2v} & \\ = & 1 & \end{array}$$

Since $(p-1)^{(p-1)/2} \equiv_p 1$, from Euler's criteria, it follows that $p - 1$ is a quadratic residue modulo p. Therefore, $x^2 \equiv_p (p-1) \;\Rightarrow\; x^2 \equiv_p -1$ has two solutions, say x_1 and x_2. We know that $x_2 = p - x_1$, and therefore, atleast

one of the solutions must be less than $p/2$. Therefore, there exists an integer $x = x_0$ satisfying $0 < x_0 < p/2$ and $x_0^2 \equiv_p -1 \;\Rightarrow\; x_0^2 + 1 \equiv_p 0$. Therefore

$$x^2 + y^2 = kp$$

has a solution $\{x_0, 1\}$ for some positive k. Note that since $x_0 < p/2$, we have $x_0^2 + 1 = p^2/4 + 1 < p^2$. Since $x_0^2 + 1^2 = kp < p^2$, it follows that $k < p$.

Consider $\{x_1, y_1\}$ such that $x_0 \equiv_k x_1$ and $y_0 \equiv_k y_1$ with $-k/2 < x_1 \leq k/2$ and $-k/2 < y_1 \leq k/2$. This is easily enforced by the observation that if $x_0 \equiv_k m$ then $x_0 \equiv_k k - m$, and if $m > k/2$ then $k - m \leq k/2$.

$$\begin{aligned} x_1^2 + y_1^2 &= (x_0 - ck)^2 + (y_0 - dk)^2 \\ &= x_0^2 - 2ckx_0 + (ck)^2 + y_0^2 - 2dky_0 + (dk)^2 \\ &= x_0^2 + y_0^2 + k(-2cx_0 + c^2k - 2dy_0 + d^2k) \\ &\equiv_k x_0^2 + y_0^2 \\ &\equiv_k 0 \end{aligned}$$

Since $x_1 \leq k/2$ and $y_1 \leq k/2$, we have $x_1^2 + y_1^2 \leq 2(k/2)^2$. Since $x_1^2 + y_1^2 \equiv_k 0 = k'k$. From the above observation we have $k'k < 2(k/2)^2 \;\Rightarrow\; k' < k$.

Note that we have a solution $\{x_0, y_0\}$ for the equation $x^2 + y^2 = kp$ where $p \equiv_4 1$ and $k < p$. The main idea of the proof is as follows: using $\{x_0, y_0\}$ and $\{x_1, y_1\}$ just described above, we will construct another pair of integers $\{x_2, y_2\}$ such that $x_2^2 + y_2^2 = jp$ with $j < k$. Hence, using a solution of $x^2 + y^2 = kp$, we get a solution to $x^2 + y^2 = jp$, with $j < k$. This reduction step can be repeated until $j = 1$, and then we have the solution to $x^2 + y^2 = 1 \cdot p$.

Observe that

$$\begin{aligned} x_0x_1 + y_0y_1 &= x_0(x_0 - ck) + y_0(y_0 - dk) \\ &= x_0^2 - x_0ck + y_0^2 - y_0dk \\ &= x_0^2 + y_0^2 + k(-cx_0 - dy_0) \\ &\equiv_k x_0^2 + y_0^2 \end{aligned}$$

Similarly,

$$\begin{aligned} x_0y_1 - x_1y_0 &= x_0(y_0 - dk) - (x_0 - ck)y_0 \\ &= x_0y_0 - x_0dk - x_0y_0 + cky_0 \\ &= k(-x_0d + cy_0) \\ &\equiv_k 0 \end{aligned}$$

Claim 26.4 *For integers i_1, i_2, i_3 and i_4, we have*

$$(i_1^2 + i_2^2)(i_3^2 + i_4^2) = (i_1i_3 + i_2i_4)^2 + (i_1i_4 - i_2i_3)^2$$

Proof: Expanding the left hand side, we get $i_1^2i_3^2 + i_1^2i_4^2 + i_2^2i_3^2 + i_2^2i_4^2$. Expanding the right hand side, we have $i_1^2i_3^2 + i_2^2i_4^2 + 2i_1i_3i_2i_4 + i_1^2i_4^2 + i_2^2i_3^2 - 2i_1i_4i_2i_3 = i_1^2i_3^2 + i_2^2i_4^2 + i_1^2i_4^2 + i_2^2i_3^2 = i_1^2i_3^2 + i_1^2i_4^2 + i_2^2i_3^2 + i_2^2i_4^2$ which is the same as the left hand side. □ Setting $i_1 = x_0$, $i_2 = y_0$, $i_3 = x_1$ and $i_4 = y_1$ in the above equation we get

$$(x_0^2 + y_0^2)(x_1^2 + y_1^2) = (x_0x_1 + y_0y_1)^2 + (x_0y_1 - x_1y_0)^2 = kp \cdot k'k = k'k^2p \tag{26.2}$$

Since $x_0x_1 + y_0y_1 \equiv_k 0$, we have $x_0x_1 + y_0y_1 = x_2k$ for some x_2 and $x_0y_1 - x_1y_0 \equiv_k 0$, we have $x_0y_1 - x_1y_0 = y_2k$ for some y_2. Plugging this in equation 26.2, we get

$$(x_2k)^2 + (y_2k)^2 = k'k^2p$$

and cancelling k^2, we get

$$x_2^2 + y_2^2 = k'p$$

Hence we have obtained an integer pair $\{x_2, y_2\}$ that is a solution to $x^2 + y^2 = k'p$ knowing a solution to $x^2 + y^2 = kp$ with $k > k'$. The result follows by successive repetition of this reduction until $k' = 1$, which is when we have a solution pair $\{x_t, y_t\}$ such that $x_t^2 + y_t^2 = 1 \cdot p$, which is what is desired.

26.5 Multiplicative Functions and Perfect Numbers

Exercise 26.5 *Define the function $\sigma(n)$ as*

$$\sigma(n) = \sum_{d|n} d$$

An integer n is called a perfect number *if $\sigma(n) = 2n$. For example for the number 6, we have $\sigma(6) = 1+2+3+6 = 2 \cdot 6 = 12$, and therefore 6 is a perfect number. Prove that all even perfect numbers are of the form $2^{p-1}(2^p - 1)$, where both p and $2^p - 1$ are both primes.*

Answer ($\Rightarrow$) If $n = 2^{p-1}(2^p - 1)$ and $2^p - 1$ is prime (note, this implies p is prime by Chapter 29, Example 2). The divisors of n are 2^i for $1 \leq i \leq (p-1)$, and $2^j(2^p - 1)$ for $1 \leq j \leq (p-1)$. Therefore we must evaluate the sum

$$\sum_{i=1}^{p-1} 2^i + \sum_{j=1}^{p-1} 2^j(2^p - 1)$$

Observe that $\sum_{i=1}^{p-1} 2^i = 2^p - 1$. Therefore, we have

$$2^p - 1 + \sum_{j=1}^{p-1} 2^j(2^p - 1)$$

$$= (2^p - 1)(\sum_{j=1}^{p-1} 2^j + 1)$$

$$= (2^p - 1)(2^p - 1 + 1)$$

$$= (2^p - 1)2^p$$

$$= 2 \cdot 2^{p-1}(2^p - 1) = 2n$$

Therefore, n is perfect.

($\Leftarrow$) For this part of the proof, we will assume that n is an even and perfect number, and show that n is of the form $2^{p-1}(2^p - 1)$. Since n is even, we can extract the largest power of 2 from n and write it as $n = 2^{k-1}n'$, where n' is an odd and $k \geq 2$.

Claim 26.5 *σ is a multiplicative function. That is*

$$(m, n) = 1 \;\Rightarrow\; \sigma(mn) = \sigma(m) \cdot \sigma(n)$$

Proof: Consider

$$\sigma(mn) = \sum_{d|mn} d$$

If $(m, n) = 1$, then a divisor d of mn can be uniquely expressed as $d = d_1 d_2$, where $d_1|m$ and $d_2|n$, and $(d_1, d_2) = 1$. Therefore, any term appearing in the expansion of $\sigma(mn)$ will appear uniquely as a product of d_1 and d_2 in $\sigma(m) \cdot \sigma(n)$ and no other terms will appear. □

Since σ is multiplicative we have

$$\begin{aligned}\sigma(n) &= \sigma(2^{k-1})\sigma(n') \\ &= (2^k-1)\sigma(n') \quad \text{(since } \sigma(2^i) = 1+2+2^2+\dots 2^i = 2^{i+1}-1) \\ &= 2n \quad \text{(by hypothesis since } n \text{ is perfect)} \\ &= 2^k n'\end{aligned}$$

Since $(2^k-1) \nmid 2^k$, it must be that $(2^k-1) \mid n'$. Therefore, we have $n' = (2^k-1)n''$. Note that

$$\sigma(n') = \frac{\sigma(n)}{(2^k-1)} = \frac{2^k n'}{(2^k-1)} = \frac{2^k(2^k-1)n''}{2^k-1} = 2^k n''$$

Note that $n'' \mid n'$. Consider

$$n' + n'' = (2^k-1)n'' + n'' = 2^k n'' = \sigma(n')$$

It follows that n' and n'' must be the only factors of n', since if that were not the case, then $\sigma(n') > n' + n''$. So $n'' = 1$ and n' is prime. Hence $n' = 2^k - 1$ and $n = 2^{k-1}(2^k-1)$. Note, once again, from Chapter 29, Example 2, that since $2^k - 1$ is prime, k must too, necessarily be prime.

Remark The only perfect numbers less than 10^6 are 6, 28, 496 and 8128. This exercise presented here characterizes even perfect numbers. It is not known if there are infinitely many perfect numbers or if any odd perfect numbers exist.

Chapter 27

Dhan Mahesh

27.1 Exercise 1

If $F_n = 2^{2^n} + 1$, $n > 1$ is a prime, then 2 is not a primitive root of F_n
Solution:
Clearly 2 is a primitive root of $5 = F_1$
since $2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1)$
$2^{2^{n+1}} \equiv_{F_n} 1$
$\implies$ $\mathbf{Order}_2(F_n) \leq 2^{n+1}$
but F_n is prime.
$\therefore \phi(F_n) = F_n - 1 = 2^{2^n}$
but we know that $2^{2^n} > 2^{n+1}, n > 1$
$\therefore$ $\mathbf{Order}_2(F_n)$ is smaller than $\phi(F_n)$.
by the definition of Primitive root, 2 can't be primitive root of F_n.

27.2 Exercise 2

Can we extend Quadratic reciprocity law for Jacobian Symbol for -ve integers with the conditions that $\left(\frac{m}{n}\right)$ exists when both m,n are odd (and positive) and $\left(\frac{m}{-n}\right) = \left(\frac{m}{n}\right)$ and $\left(\frac{a}{\pm 1}\right) = 1$?
Solution:

1. m is -ve and n is +ve
   $\left(\frac{m}{n}\right) = \left(\frac{-x}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{x}{n}\right) = (-1)^{(n-1)/2}\left(\frac{x}{n}\right)$
   & we have $\left(\frac{n}{m}\right) = \left(\frac{n}{-x}\right) = \left(\frac{n}{x}\right)$
   by Q R Thm
   $\left(\frac{x}{n}\right)\left(\frac{n}{x}\right) = (-1)^{(x-1)(n-1)/4}$
   $\therefore \left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{-(n-1)(m+1)/4+(n-1)/2} = (-1)^{(n-1)(1-m)/4}$
2. m is +ve and n is -ve
   similar as above and we would get

$\left\{ \begin{matrix} m \\ n \end{matrix} \right\} \left\{ \begin{matrix} n \\ m \end{matrix} \right\} = (-1)^{(m-1)(1-n)/4}$

3. if both m and n are -ve
   $\left\{ \begin{matrix} m \\ n \end{matrix} \right\} = \left\{ \begin{matrix} m \\ -y \end{matrix} \right\} = \left\{ \begin{matrix} m \\ -1 \end{matrix} \right\} \left\{ \begin{matrix} m \\ y \end{matrix} \right\} = \left\{ \begin{matrix} m \\ y \end{matrix} \right\} = \left\{ \begin{matrix} -x \\ y \end{matrix} \right\} = \left\{ \begin{matrix} -1 \\ y \end{matrix} \right\} \left\{ \begin{matrix} x \\ y \end{matrix} \right\} = (-1)^{(y-1)/2} \left\{ \begin{matrix} x \\ y \end{matrix} \right\}$
   $\left\{ \begin{matrix} n \\ m \end{matrix} \right\} = \left\{ \begin{matrix} n \\ -x \end{matrix} \right\} = \left\{ \begin{matrix} n \\ -1 \end{matrix} \right\} \left\{ \begin{matrix} n \\ x \end{matrix} \right\} = \left\{ \begin{matrix} n \\ x \end{matrix} \right\} = (-1)^{(x-1)/2} \left\{ \begin{matrix} y \\ x \end{matrix} \right\}$
   $\therefore \left\{ \begin{matrix} m \\ n \end{matrix} \right\} \left\{ \begin{matrix} n \\ m \end{matrix} \right\} = (-1)^{(y-1)/2}(-1)^{(x-1)/2} \left\{ \begin{matrix} x \\ y \end{matrix} \right\} \left\{ \begin{matrix} y \\ x \end{matrix} \right\} = (-1)^{(x-1)/2+(y-1)/2+(x-1)(y-1)/4} = (-1)^{(x+1)(y+1)/4} = (-1)^{(n-1)(m-1)}$

So we can see from above cases that QR Law can be extended to -ve integers also, but only when both m, n are -ve with the conditions specified.

27.3 Exercise 3

1. Prove that if p is prime and $p|a^p - b^p$ then $p^2|a^p - b^p$
2. Prove that if $a^2 \equiv_8 1$ then $a^{2^{\alpha-2}} \equiv_{2^\alpha} 1$

Solution:

1. By Fermat's Little Thm $a^p \equiv_p a$ and $b^p \equiv_p b$
   $\therefore (a^p - b^p) \equiv_p (a - b)$
   $p|(a^p - b^p)$ (given)
   $\implies p|(a - b) \therefore a = pk + b$
   $\therefore a^p - b^p = (b + kp)^p - b^p = b^p - b^p + p^p k^p + \binom{p}{1} b^{p-1} pk \ldots + \binom{p}{i} p^i k^i b^{p-i} \ldots$
   So $p^2|(a^p - b^p)$
   Hence Proved

2. **Lemma 27.1** *If p is prime and $a \equiv_{p^\alpha} b$ then $a^{p^x} \equiv_{p^{\alpha+x}} b^{p^x}$*

   Proof: Proof by Mathematical Induction
   Base cases: for $x = 0$, this is obvious
   for $x = 1$ by Fermat's Little thm $a^p \equiv_p a$ and $b^p \equiv_p b$
   $\therefore a^p \equiv_{p^{\alpha+1}} b^p$
   IH: If it is true for $x = k$ i.e $a^{p^k} \equiv_{p^{x+\alpha}} b^{p^k}$ then it is true for $x = k + 1$ also.. i.e.$a^{p^{k+1}} \equiv_{p^{x+\alpha+1}} b^{p^{k+1}}$
   $a^{p^k} \equiv_{p^{x+\alpha}} b^{p^k}$
   $a^{p^{k+1}} = a^{p^x} * a^p \equiv_b^{p^x} *a^p \equiv_p b^{p^x} * b$
   $\therefore a^{p^{k+1}} \equiv_{p^{x+\alpha+1}} b^{p^{k+1}}$
   Hence proved
   □
   $a^2 \equiv_8 1$ consider a^2 as c and $p = 2, \alpha = 3, b = 1$.. So it becomes $c \equiv_{2^3} 1$
   So by above part(1) ,$c^{2^x} \equiv_{2^{x+3}} 1^{2^x}$
   $\implies a^{2^{2^x}} \equiv_{2^{x+3}} 1$
   If we put $\alpha = 2^x + 2$ we will get the required result
   $a^{2^{\alpha-2}} \equiv_{2^\alpha} 1$

27.4 Exercise 4

Lemma 27.2 *The product of the positive integers less than m and prime to m is congruent to -1 modulo m if $m = 4, p^n$* **or** *$2p^n$ with p an odd prime , but product is congruent to $+1$ modulo m for all other moduli.*

Proof: If $m = 4$, the product $1 * 3 \equiv_4 -1$
If $m = p^n$, let t be a quadratic non residue of the odd prime p, and let a_i, where $i = 1, 2 \ldots, \phi(p^n)$, be the least positive integers forming a reduced residue system modulo p^n. Then, for each a_i, the congruence $a_i x \equiv_p t$ doesn't exists. The integers a_i are, therefore, separated into $\phi(p^n)/2$ pairs, and if P is the product of these pairs,
$P \equiv_{p^n} t^{\phi(p^n)/2}$
But $t^{(p-1)/2} \equiv_p -1$, and hence
$(t^{(p-1)/2})^{p^{n-1}} = (-1 + kp)^{p^{n-1}}$
and $t^{p^{n-1}(p-1)/2} = -1 + Mp^n$
Therefore $t^{\phi(p^n)/2} \equiv_{p^n} -1$
and $P \equiv_{p^n} -1$
If $m = 2p^n$, let s be a quadratic nonresidue modulo p, and let t satisfy both of the congruences
$x \equiv_p s$
$x \equiv_2 1$
Therefore, t is an odd quadratic nonresidue of $2p^n$, for if $x^2 \equiv_{2p^n} t$ had a solution, then $t \equiv_p s$ would be a quadratic residue of p. The congruences $a_i x \equiv_{2p^n} t$ now pair the positive integers a_i, where $i = 1, 2, \ldots, \phi(2p^n)$, that are less than $2p^n$ and prime to $2p^n$. If P represents the product of these pairs, we find that
$P \equiv_{2p^n} t^{\phi(2p^n)/2}$
But $t^{(p-1)/2} \equiv_p -1$, and thus $t^{\phi(p^n)/2} \equiv_{p^n}$. However, t is odd, and $\phi(2p^n) = \phi(p^n)$. Therefore, $P \equiv_{2p^n} -1$

If $m = 2$, the product will be 1 (hence true)

If $m = 2^u$, where $u > 2$, then -1 is a quadratic nonresidue of 2^u. Hence, the congruences $a_i x \equiv_{2^u} -1$, where the a_i range through the positive integers less than 2^u and prime to 2, separate these integers into 2^{u-2} pairs. In this case, therefore , if P again represents the product of these pairs, $P \equiv_{2^u} (-1)^{2^{u-2}} \equiv_{2^u} 1$.

Finally suppose that m doesn't in any above category.. then we would be able to write $m = 2^u p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$. Let s be a quadratic nonresidue modulo p_1, and let t satisfy both the congrueces
$x \equiv_{p_1} s$
$x \equiv_{2p_2p_3\cdots p_r} 1$
Then t is a quadratic nonresidue of m. Again, if the a_i, where $i = 1, 2 \ldots \phi(m)$ are the positive integers less than m and prime to m, then the congruences $a_i x \equiv_m t$ pair the a_i and, as before, the Product P of the a_i is such that
$P \equiv_m t^{\phi(m)/2}$
But $t^{(p_1-1)/2} \equiv_{p_1} -1$, and $t^{\phi(m)/2} \equiv_{p_1^{n_1}} -1$. However, since $\phi(p_i^{n_i})$ is even and $\phi(m) = \phi(p_1^{n_1})\phi(p_2^{n_2}) \cdots \phi(p_r^{n_r})$, $t^{\phi(m)/2} \equiv_{p_1^{n_1}} 1$
Moreover, $t = 1 + 2p_2p_3 \cdots p_r k$, so that $t^{\phi(m)/2} = (1 + 2p_2p_3 \cdots p_r k)^{\phi(m)/2}$, and $t^{\phi(m)/2} \equiv_{p_2^{n_2} p_3^{n_3} \cdots p_r^{n_r}} 1$. Furthermore, $t^{2^{u-1}} \equiv_{2^u} 1$, and thus $t^{\phi(m)/2} \equiv_{2^u} 1$. Therefore, $t^{\phi(m)/2} \equiv_m 1$, and $P \equiv_m 1$. Hence proved.
□

27.5 Exercise 5

Write down the Quadratic Residues of 13.
Solution:
To answer this, we will see two lemmas

Lemma 27.3 *The Quadratic residues of an odd prime p coincide with teh even powers of any primitive root of p.*

Proof: Consider the congruences $x^2 \equiv_p a$ with $gcd(a, p) = 1$. then if r is a primitive root of p, because the powers $r, r^2, r^3, \ldots, r^{p-1}$ form a reduced residue system modulo p, either
$a \equiv_p r^{2k}$
$or a \equiv_p r^{2k+1}$
In first case, it is evident that a is a quadratic residue of p, for $(r^k)^2 \equiv_p a$. Applying Euler's Criterion to the second case, if
$(r^{2k+1})^{(p-1)/2} \equiv_p 1$
the exponent of r must be multiple of $p-1$. But then $(2k+1)/2$ would have to be an integer, and that is impossible. Hence, in the second case a is a quadratic nonresidue of p. Thus the set of quadratic residues of p consists of the even powers of a primitive root of p.
□
13 is a odd prime and 2 is a primitive root of 13, so the quadratic residues of 13 are $2^2 \equiv_{13} 4, 2^4 \equiv_{13} 3, 2^8 \equiv_{13} 9, 2^{10} \equiv_{13} 10, and 2^{12} \equiv_{13} 1$.

Lemma 27.4 *The integers $1^2, 2^2, \ldots ((p-1)/2)^2$ are the incongruent quadratic residues of the odd prime p.*

Proof: We can say that $a^2 \equiv_p (p-a)^2$, we need only the integers $1^2, 2^2 \ldots ((p-1)/2)^2$ to determine the quadratic residues modulo p. Each of these integers is evidently a quadratic residue of p, but, more than that, no two of them are congruent modulo p, for if
$a_1^2 \equiv_p a_2^2$
then $(a_1 - a_2)(a_1 + a_2) \equiv_p 0$
and p divides at least one of $a_1 - a_2$ and $a_1 + a_2$. But since both a_1 and a_2 are positive and less than $p/2$, neither $a_1 - a_2$ nor $a_1 + a_2$ is divisible by p. These $(p-1)/2$ integers, therefore, yield all the quadratic residues of p.
□
So by the above lemma , we can say that $1^2 \equiv_{13} 1, 2^2 \equiv_{13} 4, 3^2 \equiv_{13} 9, 4^2 \equiv_{13} 3, 5^2 \equiv_{13} 12, 6^2 \equiv_{13} 10$. and the quadratic residues of 13.

Chapter 28

Mayank Kumar

28.1 GCD

Exercise 28.1 *Show that for any integers x,m and n with $m, n \geq 0$,*

$$gcd(x^m - 1, x^n - 1) = abs(x^{gcd(m,n)} - 1)$$

Solution We will prove that LHS divides RHS and RHS divides LHS. Since the two sides are both positive in sign, so this will clearly prove that LHS = RHS.
($\Longrightarrow$)
Lets assume that d is a divisor of $gcd(x^m - 1, x^n - 1)$. So, $d|x^m - 1$ and $d|x^n - 1$.
$\Rightarrow x^m \equiv 1$ (mod d) and $x^n \equiv 1$(mod d).
We can find integers u and v such that $mu + nv = g = gcd(m, n)$, then

$$x^g \equiv x^{mu+nv} \equiv (x^m)^u (x^n)^n \equiv 1^u 1^v \equiv 1(modd)$$

so $d|abs(x^g - 1)$.
($\Longleftarrow$)
Conversely suppose that $d|x^g - 1$. Then $x^g \equiv 1$ (mod d), so $x^m \equiv (x^g)^{m/g} \equiv 1$(mod d). Similarly, $x^n \equiv 1$(mod d). So d divides both $x^m - 1$ and $x^n - 1$, and hence divides $gcd(x^m - 1, x^m - 1)$.
Hence proved.

28.2 Fibonacci Numbers

Exercise 28.2 *Show that if the Fibonacci number F(n) is prime then n is prime. More precisely prove the implication*

$$m|n \Rightarrow F(m)|F(n)$$

Solution First of all lets prove that

$$m|n \Rightarrow F(m)|F(n)$$

using the principle of induction on $l = \frac{n}{m}$
Base case Base Case is trivial, since $m = n \Rightarrow F(m)|F(n)$
Propogation Step Let us assume that the claim is true for l = k.

To Prove Claim is also true for l = k+1
Proof

$$\begin{aligned} k+1 &= \frac{n}{m}+1 \\ &= \frac{n+m}{m} \end{aligned}$$

So, it only remains to prove that if $F(m)|F(n)$ then $F(m)|F(n+m)$
Let $F(n) = p * F(m)$

$$\begin{aligned} F(n+m) &= F(n-1) * F(m) + F(n) * F(m+1) \\ &= F(m)(F(n-1) + p * F(m+1)) \end{aligned}$$

Hence proved.
If F(n) is prime, then there exists no m such that $m|n$, otherwise from the above proof we would have $F(m)|F(n)$. Hence n is also a prime.

28.3 Euler's Phi Function

Exercise 28.3 *Prove that $\phi(n)$ is even for any $n \geq 3$*

Solution
Approach 1: We know that, $\phi(n)$ counts the number of integers $m, 1 \leq m \leq n-1$ which are relatively prime to n.
Claim If m is relatively prime to n, then so is $n-m$.
Proof Let us assume that there is a $k > 1$ such that $k|(n-m)$ and $k|n$. This would imply that $k|(n-(n-m))$, or simply $k|m$, which in turn says that $gcd(m,n) \geq k > 1$, which is a contradiction.
Therefore the numbers m, $1 \leq m \leq n-1$ which are relatively prime to n come in pairs $(m, n-m)$. It is clear that $m \neq n-m$, otherwise $n = 2 \times m$, and n is not relatively prime to m. Hence the number $\phi(n)$ is even.
Approach 2: Consider,

$$\begin{aligned} [1]_n^2 &= [1]_n \\ [n-1]_n^2 &= [-1]_n^2 \\ &= [1]_n \end{aligned}$$

If $n \geq 3, [-1]_n \neq [1]_n$
Also $[-1]_n, [1]_n$ form a subgroup of the group $< G_n, 1, \times >$ of order 2.
So, by Lagrange's theorem we have $2|o(G_n) = \phi(n)$, i.e $\phi(n)$ is even.

28.4 Chinese Remainder Theorem

Exercise 28.4 *Argue that, under the definitions of Chinese Remainder Theorem, if gcd(a,n)=1, then*

$$(a^{-1} mod n) \leftrightarrow ((a_1^{-1} mod n_1), (a_2^{-1} mod n_2), ..., (a_k^{-1} mod n_k))$$

Solution From Chinese Remainder Theorem, we know that

$$(a mod n) \leftrightarrow ((a mod n_1), (a mod n_2), ..., (a mod n_k))$$

Since, gcd(a,n) = 1, they are relatively prime, and hence $a^{-1} mod n$ is defined. Similarly $a^{-1} mod n_i$ is also defined. Now substituing a^{-1} in place of a in the above relationwe get,

$$(a^{-1} mod n) \leftrightarrow ((a^{-1} mod n_1), (a^{-1} mod n_2), ..., (a^{-1} mod n_k))$$

It remains to prove that,

$$(a_i^{-1} mod n_i) = (a^{-1} mod n_i)$$

Consider,

$$
\begin{aligned}
a * (a_i^{-1} mod n_i)(mod n_i) & \\
&= (a_i * a_i^{-1})(mod n_i) \\
&= 1(mod n_i)
\end{aligned}
$$

Hence,

$$(a^{-1} mod n) \leftrightarrow ((a_1^{-1} mod n_1), (a_2^{-1} mod n_2), ..., (a_k^{-1} mod n_k))$$

28.5 Jacobi Symbol

Exercise 28.5 *Let $n \geq 1$ be an odd integer. Calculate the Jacobi symbol*

$$(\frac{5}{3 \times 2^n + 1})$$

Solution Since $5 \equiv 1$ mod 4, the quadratic reciprocity law gives

$$(\frac{5}{3 \times 2^n + 1}) = (\frac{3 \times 2^n + 1}{5})$$

To determine the value of $3 \times 2^n + 1$ modulo 5, we distinguish the cases $n \equiv 1$ mod 4 and $n \equiv 3$ mod 4.

- **Case $n \equiv 1$ mod 4** Then n = 4k + 1 with an integer k ≥ 0 and

  $$3.2^n = 3.2^{4k+1} = 3.2.(2^4)^k = 6.16^k \equiv 1.1^k \equiv 1 mod 5$$

  hence

  $$(\frac{3 \times 2^n + 1}{5}) = (\frac{1 + 1}{5}) = (\frac{2}{5}) = -1$$

- **Case $n \equiv 3$ mod 4** Then n = 4k + 3 with an integer k ≥ 0 and

  $$3.2^n = 3.2^{4k+3} = 3.2^3.(2^4)^k = 24.16^k \equiv (-1).1^k \equiv -1 mod 5$$

  hence

  $$(\frac{3 \times 2^n + 1}{5}) = (\frac{-1 + 1}{5}) = (\frac{0}{5}) = 0$$

Chapter 29

Hitesh Chaudhary

29.1 Fermat's Little Theorem

Exercise 29.1 *Show* $7 \mid 2222^{5555} + 5555^{2222}$

Solution: By FLT, $n^7 \equiv_7 n$.
So for natural numbers q and r, $n^{7q+r} \equiv_7 (n^7)^q.n^r \ \equiv_7 \ n^q.n^r \ \equiv_7 n^{q+r}$
Now, $2222 \equiv_7 3$ and $5555 \equiv_7 4 \equiv_7 -3$.

$$
\begin{aligned}
\text{Thus } 2222^{5555} + 5555^{2222} &\equiv_7 3^{5555} + (-3)^{2222} \\
&\equiv_7 3^{793+4} + (-3)^{317+3} \\
&\equiv_7 3^{113+6} + (-3)^{45+5} \\
&\equiv_7 3^{17+0} + (-3)^{7+1} \\
&\equiv_7 3^{2+3} + (-3)^{1+1} \\
&\equiv_7 3^2(3^3+1) \\
&\equiv_7 3^2.28 \equiv_7 0
\end{aligned}
$$

□

29.2 Tchebychev's Theorem

Exercise 29.2 *Let* β *be the positive real number less than 1. Show if the integer* N *is very large enough, there exist a prime between* βN *and* N.

Solution: Lets $\beta < 1$. By Tchebychev's Theorem, $\pi(n) \sim \frac{n}{\log n}$ and $\pi(\beta n) \sim \frac{\beta n}{\log \beta n} \sim \frac{\beta n}{\log n + \log \beta} \sim \frac{\beta n}{\log n}$
Therefore, for sufficiently large n, $\pi(n) > \pi(\beta n)$. Hence there is atleast one prime between βn and n. □

29.3 Prime Numbers

Exercise 29.3 *Show that* $a^2 + b^2 + c^2 + d^2$ *is never prime.*

Solution: Any composite number *C can always be written as a product in atleast 2 ways. (As 1.C is always possible). Lets* $C = ab = cd$ *then* $C \mid ab$*. Set* $c = mn$ *such thatm is part which divides a and n is the part which divides b. Then there are p and q such that*
$a = mp$, $b = nq$

Solving $ab = cd$ *for* d *gives,* $d = \frac{ab}{c} = \frac{(mp)(nq)}{mn} = pq$. *It then follows that*

$S = a^2 + b^2 + c^2 + d^2$
$= m^2p^2 + n^2q^2 + m^2n^2 + p^2q^2$ *It therefore follows that* $a^2 + b^2 + c^2 + d^2$ *can never be prime.*
$= (m^2 + q^2)(n^2 + p^2)$

□

29.4 Congruences

Exercise 29.4 *f(x) of degree k and* $f(x) \equiv 0$ *(mod p) have k solutions. and* $f(x) = f_1(x)f_2(x)$ *. Then number of incongruent solutions of* $f_1(x) \equiv 0$*(mod p) is equal to its degree and similarly for* $f_2(x)$

Solution: Let $f_1(x) = b_0x^l + ... + b_l$ and $f_2(x) = c_0x^m + ... + c_m$ where $b_0 \not\equiv 0c_0 \not\equiv 0$(mod p) . Then, $f(x) = b_0c_0x^{l+m} + ... + b_lc_m$(mod p), l+m = k Each solution of $f(x) \equiv 0$ (mod p) will be solution of at least one of the congruences, $f_1(x) \equiv 0$(mod p) or $f_2(x) \equiv 0$(mod p) . Conversely is also true.
Now if number of incongruent solutions of $f_1(x) \equiv 0$ (mod p) or $f_2(x) \equiv 0$(mod p) were less than respectively l or m, then numbfer of solutions of $f(x) \equiv 0$(mod p) would be less than l+m = k which is contrary to hypothesis. Thus $f_1(x) \equiv 0$(mod p) must have *l solutions and* $f_2(x) \equiv 0$*(mod p) must have m solutions.* □

29.5 Continued Fractions

Exercise 29.5 *If a is vlaue of continued fraction* $< a_0; a_1, ... >$ *and* $r_n = \frac{P_n(a_0,a_1,...,a_n)}{Q_n(a_0,...,a_n)}$ *is* n^{th} *partial quotient then,* $\frac{1}{2Q_nQ_{n+1}} < |a - \frac{P_n}{Q_n}| < \frac{1}{Q_nQ_{n+1}} < \frac{1}{Q_n^2}$

Solution: As proved in lecture,
for k = -1, 0, ... we have $P_{k+1}Q_k - Q_{k+1}P_k = (-1)^k$, $P_{k+2}Q_k - Q_{k+2}P_k = (-1)^k x_{k+2}$
Also, if r_n denotes n^{th} partial quotient then for each n , $r_{2n} < r_{2n+2}$ and $r_{2n+1} < r_{2n-1}$ and for all m, n, $r_{2m} < r_{wn+1}$

from above assertions we have,
$|a - \frac{P_n}{Q_n}| \leq |\frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n}| = \frac{1}{Q_nQ_{n+1}} < \frac{1}{Q_n^2}$ because $Q_{n+1}(a_0, ..., a_{n+r}) = a_{n+1}Q_n(a_0, ..., a_n) + Q_{n-1}(a_0, ..., a_n) > Q_n(a_0, ..., a_n)$
Similarly, $|a - \frac{P_n}{Q_n}| = |\frac{P_{n+2}}{Q_{n+2}} - \frac{P_n}{Q_n}| = \frac{a_{n+2}}{Q_nQ_{n+2}} = \frac{a_{n+2}}{Q_n(a_{n+2}Q_{n+1}Q_{n+1}+Q_n)} \geq \frac{1}{Q_n(Q_n+Q_{n+1})} > \frac{1}{2Q_nQ_{n+1}}$

□

Chapter 30

Satish Parvataneni

30.1 CRT

Theorem 30.1 *Show that* $\exists x$ *for any* n *such that* $x+1, x+2, \ldots, x+n$ *are composit numbers.*

Proof: Given any n, from the fact the primes are infinite we can list out n prime numbers $p_1, p_2, \ldots, p_n$.

Fact 30.2 *By CRT for any* $m_1, m_2, \ldots, m_r$ *pair wise relatively prime numbers the system of equations*

$$x \equiv_{m_i} a_i where 1 \leq i \leq r \tag{30.1}$$

has a unique solution modulo M *where* $M = \prod_{i=1}^{r} m_i$

so for $p_1, p_2, \ldots, p_n$ primes (which are pair wise relatively prime numbers) we can find out an x which satisfies the system of equations Eqn. 30.1 for $a_1 = -1, a_2 = -2, \ldots, a_n = -n$.

System of equations become

$$x \equiv_{p_i} a_i \tag{30.2}$$

where $1 \leq i \leq n$ and $a_1 = -1, a_2 = -2, \ldots a_n = -n$.

From the above system of equations we can conclude that $p_1|x+1, p_2|x+2, \ldots, p_n|x+n$ and hence proved. □

30.2 FLT

Theorem 30.3 *if* p *and* q *are distinct primes, prove that* $p^{q-1} + q^{p-1} \equiv 1 \mod pq$

Proof:

Fact 30.4 *By FLT if* p *is a prime and* $p \not| a$ *then* $a^{p-1} \equiv 1(\mod p)$

As p and q are distinct primes $p \not| p$ and $q \not| p$ by FLT

$$p^{q-1} \equiv 1 \mod q \tag{30.3}$$

$$q^{p-1} \equiv 1 \mod p \tag{30.4}$$

As $p^{q-1}|p$ and $q^{p-1}|q$ are trivially true we can write

$$q^{p-1} \equiv 0 \mod q \tag{30.5}$$

$$p^{q-1} \equiv 0 \mod p \tag{30.6}$$

From Eqn. 30.3 and Eqn. 30.5

$$p^{q-1} + q^{p-1} \equiv 1 \mod q \tag{30.7}$$

and From Eqn. 30.4 and Eqn. 30.6

$$p^{q-1} + q^{p-1} \equiv 1 \mod p \tag{30.8}$$

Theorem 30.5 *if* $a \equiv b \mod n_1$ *and* $a \equiv b \mod n_2$ *and* $gcd(n_1, n_2) = 1$ *then* $a \equiv b \mod n_1 n_2$

Proof: Let c=a-b then $n_1|c$ and $n_2|c$, integers r and s can be found such that $c = rn_1 = sn_2$.
Given $gcd(n_1, n_2) = 1$ allows us to write $1 = xn_1 + yn_2$ for some choice of integers x and y.Multiplying the last equation by c then

$$c = c * 1 = c(n_1 x + n_2 y) = n_1 cx + n_2 cy. \tag{30.9}$$

If appropriate substitutions are now made on the right hand side, then

$$c = n_1(sn_2)x + n_2(rn_1)y = n_1 n_2(sx + ry) \tag{30.10}$$

Substituting c=a-b in the above equation we get $a \equiv b \mod n_1 n_2$ and hence proved.

□

From the above fact and Eqn. 30.7 and Eqn. 30.8 we can conclude that

$$p^{q-1} + q^{p-1} \equiv 1 \mod pq \tag{30.11}$$

□

30.3 GCD

Theorem 30.6 *Prove that gcd of two postive integers always divide their LCM*

Proof: Let a and b be any two positive integers, d is the gcd(a,b) and l is the lcm(a,b), By definition

$$l = ak_1 = bk_2.$$
$$d|a \text{ and } d|b \text{ ie } a = dc_1 \text{ and } b = dc_2$$

if we find gcd(d,l) it reduces to $gcd(d, ak_1)$ and on further reduction $gcd(d, dc_1 k_1)$ hence gcd(d,l) comes out to be d and hence $d|l$. □

30.4 Linear Congruences

Theorem 30.7 *if $x \equiv a \mod n$ prove that either $x \equiv a \mod 2n$ or $x \equiv a + n(\mod 2n)$*

Proof:

$$x - a = kn \quad from \quad x \equiv a \mod n \tag{30.12}$$

$$x - a = k_1 2n + r \quad on\ dividing\ kn\ by\ 2n\ where\ 0 \le r < 2n \tag{30.13}$$

$$k_1 2n + r = kn \tag{30.14}$$

$$r = kn - k_1 2n \tag{30.15}$$

$$r = n(k - 2k_1) \tag{30.16}$$

As $0 \le r < 2n$ the value of $k - 2k_1$ can be either 0 or 1.

- when $k - 2k_1$ is zero then the value of r is zero and hence Eqn. 30.13 reduces to $x - a = k_1 2n$ which is equal to $x \equiv a \mod 2n$
- when $k - 2k_1$ is one then the value of r is n and hence Eqn. 30.13 reduces to $x - a = k_1 2n + n$ which is equal to $x \equiv a + n \mod 2n$

□

30.5 Primes

Theorem 30.8 *if $p \ge 5$ is a prime number ,show that $p^2 + 2$ is composite*

Proof: In order to prove the above we first prove a general result.

Theorem 30.9 *Any prime number number greater than 3 has a remainder 1 or 5 when divided by 6*

Proof: Any integer n can be represented in the following form.

$$n = 6 * q + r \quad where 0 \le r < 6. \tag{30.17}$$

Hence we have 6 choices for r : 0, 1, 2, 3, 4, 5. From the fact that n is a prime and therefore it is not divisible by 2 or 3 we can analyze these 6 choices.

1. r is 0 then n=6*q and clearly it is divisible by 2 which is not possible since n is a prime.
2. r is 1 then it is possible.
3. r is 2 then n=6*q+2 and clearly it is divisible by 2 which is not possible since n is a prime.
4. r is 3 then n=6*q+3 and clearly it is divisible by 3 which is not possible since n is a prime.
5. r is 4 then n=6*q+4 and clearly it is divisible by 2 which is not possible since n is a prime.
6. r is 5 then it is possible.

we can see that the only possible remainders for n divided by 6 are 1 and 5. □

Hence any prime $p \geq 5$ can be in one of the forms 6k+1 or 6k+5.

- if p is of 6k+1 form then $p^2 + 2 = 6k + 1^2 + 2$ which reduces to $36k^2 + 12k + 3$ which is clearly divisible by 3 and hence it is composite.
- if p is of 6k+5 form then $p^2 + 2 = 6k + 5^2 + 2$ which reduces to $36k^2 + 60k + 27$ which is clearly divisible by 3 and hence it is composite.

□

Chapter 31

Bipin Tripathi

31.1 Euler ϕ function, FLT

Example Let m > 1 and n > 1, Prove that $\phi(m*n) = \frac{\phi(m)\phi(m)gcd(m,n)}{\phi(gcd(m,n))}$

Proof
case 1 If gcd(m,n) = 1 and ϕ is a multiplicative function then

$\phi(m*n) = \phi(m)*\phi(n) = \frac{\phi(m)\phi(m)gcd(m,n)}{\phi(gcd(m,n))}$

case 2 if gcd(m,n) $\neq$ 1 then
Let d = gcd(m,n) = $p_1^{a_1}\ldots\ldots p_t^{a_t}$, $a_1 \geq 1,\ldots\ldots,a_t \geq 1$
and m = $p_1^{b_1}\ldots\ldots p_t^{b_t}$ M n = $p_1^{c_1}\ldots p_t^{c_t}$ N (Where gcd(M,N) = 1) and $p_1,\ldots,p_t$ do not divide MN. Hence $m*n = p_1^{b_1+c_1}\ldots p_t^{b_t+c_t}M*N$,
$\phi(m*n) = \phi(p_1^{b_1+c_1})\ldots\ldots\phi(p_t^{b_t+c_t})\phi(M)*\phi(N)$
since $\phi(p^k) = p^k(1-1/p)$
$\phi(m*n) = p_1^{b_1+c_1-1}(p_1-1)\ldots\ldots p_t^{b_t+c_t-1}(p_t-1)\phi(M)*\phi(N)$
now,
$\frac{\phi(m)\phi(n)d}{\phi(d)} = \frac{\phi(p_1^{b_1})......\phi(p_t^{b_t})\phi(M)\phi(p_1^{c_1})......\phi(p_t^{c_t})\phi(N)(p_1^{a_1}......p_t^{a_t})}{\phi(p_1^{a_1})......\phi(p_t^{a_t})}$

$\frac{\phi(m)\phi(n)d}{\phi(d)} = \frac{p_1^{b_1-1}(p_1-1)......p_t^{b_t-1}(p_t-1)\phi(M)p_1^{c_1-1}(p_1-1)......p_t^{c_t-1}(p_t-1)\phi(N)(p_1^{a_1}......p_t^{a_t})}{p_1^{a_1-1}(p_1-1)......p_t^{a_t-1}(p_t-1)}$

$\frac{\phi(m)\phi(n)d}{\phi(d)} = p_1^{b_1+c_1-1}(p_1-1)\ldots\ldots p_t^{b_t+c_t-1}(p_t-1)\phi(M)*\phi(N)$

$\frac{\phi(m)\phi(n)d}{\phi(d)} = \phi(m*n)$

31.2 Congruences of higher degree

Example Show that the congruence $x^2 \equiv 1(mod 2^k)$ has exactly four solutions mod 2^k, namely $x \equiv \pm 1$ or $x \equiv \pm(1+2^{k-1})(mod 2^k)$, when $k \geq 3$.Show that when $k = 1$ there is one solution and when $k = 2$ there are two solutions mod 2^k.

Proof
Let $x^2 \equiv 1(mod 2^k)$ then $2^k | x^2 - 1 \Rightarrow 2^k | (x-1)(x+1)$

since $gcd((x-1),(x+1)) = 2 \Rightarrow gcd((x-1)/2,(x+1)/2) = 1$, for $k \geq 3$ $2^{k-2}|((x-1)/2*(x+1)/2)$ and also as $k-2 \geq 1 \Rightarrow 2|((x-1)/2*(x+1)/2)$

Case 1 if $2|(x-1)/2$ then 2 does not divide $(x+1)/2$ so we get $2^{k-2}|(x-1)/2 \Rightarrow 2^{k-1}|(x-1)$
Hence $x \equiv 1(mod 2^{k-1})$ or equivalently x $\equiv 1$ or $1+2^{k-1}(mod 2^k)$

Case 2 if $2|(x+1)/2$ then similarily the case1 we can get x $\equiv -1$ or $-(1+2^{k-1})(mod 2^k)$

Conversely , suppose x $\equiv \pm 1$ or $\pm(1+2^{k-1})(mod 2^k)$
then x $\equiv \pm 1(mod 2^{k-1}) \Rightarrow x = \pm 1 + K2^{k-1}$,
Hence $x^2 = 1 \pm 2K*2^{k-1} + (K2^{k-1})^2$
$= 1 \pm K*2^k + K^2*2^{2k-2}$
$\equiv 1(mod 2^k)$ as $2k-2 \geq k$

Now for k=1 ,
$x^2 \equiv 1$ (mod 2) has solution x $\equiv$ 1(mod 2)
Now for k=2 ,
$x^2 \equiv 1$ (mod 4) has solution x $\equiv \pm 1$ (mod 4)

31.3 Quadratic Irrational

Example Let $d = a^2 + b$, where a,b $\in N, b > 1$ and $b|2a$.Prove that $[\sqrt{d}] = a$ and that $\sqrt{d}$ has the continued fraction expression

$$\sqrt{d} = [a, \overline{\tfrac{2a}{b}, 2a}]$$

Hence , or otherwise , derive the continued fraction expression for $\sqrt{D^2 - D}$, when $D > 2$ is a postive integer. Conversely, if the continued fraction expression of $\sqrt{d}$ has period length 2, show that $d = a^2 + b$, where a,b $\in N, b > 1$ and $b|2a$.

Proof
Let $d = a^2 + b$, where a,b $\in N$, $b > 1$ and $b|2a$
$a^2 < d \leq a^2 + 2a < (a+1)^2$
$\Rightarrow a < \sqrt{d} < a+1$ and $a = [\sqrt{d}]$
Now $x_0 = \sqrt{d}$, $p_0 = 0$, $q_0 = 1$, $a_0 = [\sqrt{d}] = a$
$x_i = \frac{p_i + \sqrt{d}}{q_i}$, $p_{i+1} = a_i * q_i - p_i$, $q_{i+1} = \frac{d - p_{i+1}^2}{q_i}$
$p_1 = a_0 * q_0 - p_0 = a*1 - 0 = a$, $q_1 = \frac{d - p_1^2}{q_0} = \frac{a^2+b-a^2}{1} = b$, $x_1 = \frac{p_1+\sqrt{d}}{q_1} = \frac{a+\sqrt{a^2+b}}{b}$, $a_1 = [x_1] = 2a/b$
,
$p_2 = \frac{2a}{b}b - a = a$, $q_2 = \frac{a^2+b-a^2}{b} = 1$, $x_2 = \frac{a+\sqrt{a^2+b}}{1}$, $a_2 = [x_2] = 2a$,
$p_3 = 2a*1 - a = a$, $q_3 = \frac{a^2+b-a^2}{1} = b$, $x_3 = \frac{a+\sqrt{a^2+b}}{b} = x_1$
Hence $\sqrt{d} = \sqrt{a^2+b} = [a, \overline{\frac{2a}{b}, 2a}]$
Next , Let $D > 2$, , D $\in$ N then $D^2 - D = (D-1)^2 + (D-1)$, and $D-1|2(D-1)$
Hence $\sqrt{D^2 - D} = [D-1, \overline{2, 2D-2}]$
Conversely, the continued fraction expression of $\sqrt{d}$ has period length 2,
before going further, let take following theorem :
Theo. : If postive integer d is not a perfect square , the simple continued fraction expression of $\sqrt{d}$ has the form

$$\sqrt{d} = [a_0, \overline{a_1, a_2, \ldots\ldots a_{r-1}, 2a_0}] \qquad \text{with } a_0 = [\sqrt{d}]$$

So for $[a_0, \overline{a_1, 2a_0}] = a_0 + x^{-1}$ so that $x = [\overline{a_1, 2a_0}]$, observing that $x = [a_1, 2a_0, \overline{a_1, 2a_0}] = [a_1, 2a_0, x]$
we get $x = a_1 + (2a_0 + x^{-1})^{-1}$, solving this for x^{-1} and discarding the negative solution, we get $x^{-1} = a_0 + \sqrt{d}$
So instead of solving x^{-1} take another way
Suppose $\sqrt{d} = [a_0, \overline{a_1, 2a_0}]$, $a_1 \neq 2a_0$
then $x = a_0 + \sqrt{d} = [\overline{2a_0, a_1}] = 2 * a_0 + \frac{1}{a_1 + \frac{1}{x}} = 2a_0 + \frac{x}{a_1 x + 1}$
Hence $a_1 x^2 + x = 2a_0 a_1 x + 2a_0 + x$
$a_1 x^2 = 2a_0 a_1 x + 2a_0$
$\Rightarrow \quad a_1(a_0^2 + 2\sqrt{d}a_0 + d) = 2a_0 a_1(a_0 + \sqrt{d}) + 2a_0$
$\Rightarrow \quad a_1 d = a_0^2 a_1 + 2a_0$
$\Rightarrow \quad d = a_0^2 + \frac{2a_0}{a_1} = a^2 + b$
where a = a_0 and $b = \frac{2a_0}{a_1} \neq 1$ here $b \in N$

31.4 Congruence, Euclidian Algorithm

Example
(a) If a ≥ 1 , b ≥ 1 , prove that gcd($2^a - 1, 2^b - 1) = 2^{gcd(a,b)} - 1$.
(b) Prove that gcd(a,b)=gcd(a+bc,b) for any integers a , b ,and c.

(a) Proof
Let a ≥ 1 , b ≥ 1 and $d = gcd(a, b)$ and $e = gcd(2^a - 1, 2^b - 1)$
then $d|a$, $d|b$ and $e|2^a - 1$, $e|2^b - 1$
now $2^d - 1|2^a - 1$,$2^d - 1|2^b - 1$ so $2^d - 1|e$
Assume $d = gcd(a, b) = ax - by$, where x and y are postive integers.
also $2^a \equiv$1 (mod e), so $2^{ax} \equiv$1 (mod e)
similarly $2^b \equiv$1 (mod e), so $2^{by} \equiv$1 (mod e)
Hence $2^{ax} \equiv 2^{by}$ (mod e) $\Rightarrow 2^{ax-by} * 2^{by} \equiv 2^{by}$(mod e)
Hence $2^{ax-by} \equiv 1$ (mod e) $\Rightarrow e|2^d - 1$
since $2^d - 1|e$ and $e|2^d - 1$ then e = $2^d - 1 \Rightarrow gcd(2^a - 1, 2^b - 1) = 2^{gcd(a,b)} - 1$.

(b) Proof
We first show that the common divisors of a and b is identical to the set of common divisors of a+bc and b. For if d divides a and b then it divides bc and hence a+bc , while if d divides a + bc and b then it divides bc and hence (a+bc) - bc = a. Now gcd(a,b) is a common divisor of a and b , so by the above it is acommon divisor of a+bc and b, so it divides gcd(b,a+bc) by definition of gcd(b,a+bc) . Similarly , gcd(b,a+bc) divides gcd(a,b). So gcd(a,b) = ± gcd(b,a+bc), but since both gcd(a,b) and gcd(b,a+bc) are nonnegative ,by definition ,therefore

gcd(a,b)= gcd(b,a+bc)

31.5 Primitive Roots

Example For an odd prime p show that there are as many primitive roots of $2p^n$ as of p^n.

Proof
($\Rightarrow$) Let r is primitive root of $2p^n$, by definition of primitive roots : if r is primitive root of $2p^n$ then $r^{\phi(2p^n)} \equiv_{2p^n} 1$ and $r^k \not\equiv_{2p^n} 1$ for all postive integers $k < \phi(2p^n)$ hence gcd$(r, 2p^n)$ =1
Now $\phi(2p^n) = \phi(p^n)$ since p is odd prime and $r^{\phi(2p^n)} \equiv_{2p^n} 1$
then $r^{\phi(p^n)} \equiv_{2p^n} 1$ and we have gcd(r, p^n) =1 because gcd$(r, 2p^n)$ =1
we claim r is a primitive root of p^n,

Assume r is not primitive root of p^n, then there is a $k < \phi(p^n)$ such that $r^k \equiv_{p^n} 1 \Rightarrow p^n | r^k - 1$ and also r is such that $\gcd(r, 2p^n) = 1$
so r^k is odd because $2p^n$ will be even $\Rightarrow r^k - 1$ is even and also p^n is odd.
when we say $p^n | r^k - 1$ (i.e. an odd number is dividing an even number) so $2p^n$ should also divide $r^k - 1$, hence $2p^n | r^k - 1 \Rightarrow r^k \equiv_{2p^n} 1$
since $\phi(p^n) = \phi(2p^n)$ and $k < \phi(p^n)$ then r is not primitive root of $2p^n \Rightarrow$ Contradiction
$\Rightarrow$ r is of primitive root of p^n
Hence if r is primitive root of $2p^n$ then r is also primitive root of p^n

($\Rightarrow$) Let r is primitive root of p^n. either r is an odd integer or even integer (if r is even, then $r + p^n$ is odd and is still a primitive root of p^n). Then $\gcd(r, 2p^n)$ =1.
The order m of r modulo $2p^n$ must divide $\phi(2p^n) = \phi(p^n)$
But $r^m \equiv_{2p^n} 1$ implies that $r^m \equiv_{p^n} 1$, and so $\phi(p^n)|m$. Together these divisibility conditions forces $m = \phi(2p^n)$ making r a primitive root of $2p^n$.
Hence if r is primitive root of p^n then r is also primitive root of $2p^n$
So for an odd prime p, there are as many primitive roots of $2p^n$ as of p^n.

Chapter 32

Amit Agarwal

32.1 Example 1

Example 32.1 *Show that the Carmichael numbers are square-free and the product of atleast three primes.*

Proof: Suppose for contradiction that $p^2|n$. Let g be a generator modulo p^2, i.e., an integer s.t. $g^{p(p-1)}$ is the lowest power of g which is $\equiv_{p^2} 1$. (it is easily proved that such a g always exists.)
Let n' be the product of all primes other than p which divide n. By the Chinese Remainder Theorem, there is an integer b satisfying the two congruences:

$$b \equiv_{p^2} g \tag{32.1}$$

and

$$b \equiv_{n'} 1. \tag{32.2}$$

Then b is like g, a generator modulo p^2, and it also satisfies $\gcd(b, n) = 1$, since it is not divisible by p or any prime which divides n'. We claim that n is not a pseudoprime to the base b. To see this, we notice that if $b^{n-1} \equiv_n 1$ holds, then, since $p^2|n$, we automatically have $b^{n-1} \equiv_{p^2} 1$. But in that case $p(p-1)|n-1$, since $p(p-1)$ is the order of b modulo p^2. However, $n-1 \equiv_p -1$, since $p|n$, and this means that $n-1$ is not divisible by $p(p-1)$. This contradiction proves that there is a base b for which n fails to be a pseudoprime.

Lemma 32.1 *If n is square free, then n is a Carmichael number iff $p-1|n-1$ for every prime p dividing n.*

Proof: First Suppose that $p-1|n-1$ for every p dividing n. Let b be any base, where $\gcd(b, n) = 1$. Then for every prime p dividing n we have: b^{n-1} is a power of b^{p-1}, and so

$$b^{n-1} \equiv_p 1. \tag{32.3}$$

Thus, $b^{n-1} - 1$ is divisible by all of the prime factors p of n, and hence by their product, which is n. Hence,

$$b^{n-1} \equiv_n 1 \forall b. \tag{32.4}$$

Conversely, suppose that there is a p s.t. $p-1$ does not divide $n-1$. Let g be an integer which generates $\mathbf{Z}_p^*$. Find an integer b which satisfies:

$$b \equiv_p g \tag{32.5}$$

$$b \equiv_{\frac{n}{p}} 1. \tag{32.6}$$

Then

$$\gcd(b,n) = 1 \quad (32.7)$$
$$b^{n-1} \equiv_p g^{n-1}. \quad (32.8)$$

But $g^{n-1} \not\equiv_p 1$, because $n-1$ is not divisible by the order modulo $p-1$ of g. Hence, $b^{n-1} \not\equiv_p 1$, and so n is not prime. □ Now it remains to rule out the possibility that $n = pq$ is the product of two distinct primes. Suppose that $p \le q$. Then, if n were a Carmichael number, we would have $n-1 \equiv_{q-1} 0$, by lemma 32.1. But

$$n-1 = p(q-1+1)-1 \quad (32.9)$$
$$\equiv_{q-1} p-1 \quad (32.10)$$
$$\not\equiv_{q-1} 0 \quad (32.11)$$

since $0 \le p-1 \le q-1$. This concludes the proof. □

32.2 Example 2

Definition 32.1 *A prime of the form $2^n - 1$ is called a Mersenne prime. An interesting theorem relating to Mersenne primes is that if $2^n - 1$ is a prime, then, so is n.*

Example 32.2 *Let p be a Mersenne prime, let $q = p^2$, and let i be a root of $X^2+1=0$, so that $\mathbf{F}_p = \mathbf{F}_{p(i)}$. Suppose that the integer a^2+b^2 is a generator of $\mathbf{F}_p^*$. Prove that $a+bi$ is a generator of $\mathbf{F}_q^*$.*

Proof: We have

$$(a+bi)^{p+1} = (a^p + b^p i^p)(a+bi) \quad (32.12)$$
$$= (a-bi)(a+bi) \quad (32.13)$$
$$= a^2+b^2. \quad (32.14)$$

Claim 32.1 *If $(a+bi)^m \in \mathbf{F}_p$, then $p+1|m$.*

Proof: Let

$$d = \gcd(m, p+1). \quad (32.15)$$

We see that

$$(a+bi)^d \in \mathbf{F}_p. \quad (32.16)$$

But since $p+1$ is a power of 2, if $d \le p+1$ we find that $(a+bi)^{\frac{p+1}{2}}$ is an element of $\mathbf{F}_p$ whose square is a^2+b^2.

Claim 32.2 *a^2+b^2 is not a residue.*

Proof: Any power of a residue is a residue, so none of the nonresidues can occur as a power. □ Hence, $d = p+1$ and $p+1|m$. □ Now, suppose that

$$n = n'(p+1) \quad (32.17)$$

is such that $(a+bi)^n = 1$ (note that $p+1|n$ by the claim).
Then

$$(a^2+b^2)^{n'} = 1. \quad (32.18)$$

So $p-1|n'$ because a^2+b^2 is a generator of $\mathbf{F}_p^*$. □

32.3 Example 3

Example 32.3 *Let $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ be an odd integer, and suppose that a is prime to m and is the square of some integer modulo m. Find x s.t. $x^2 \equiv_m a$. Suppose that for each j you know a nonresidue modulo p_j, i.e., an integer n_j s.t. $\left(\frac{n_j}{p_j}\right) = -1$. For each fixed $p = p_j$ suppose you know some x_0 s.t. $x_0^2 \equiv_p a$. Show how you can then find some $x = x_0 + x_1 p + \ldots + x_{\alpha-1} p^{\alpha-1}$ s.t. $x^2 \equiv_p^\alpha a$.*

Proof: We use induction on α.

To go from $\alpha - 1$ to α, suppose you have an $(\alpha - 1)$-digit base-p integer x' s.t.

$$x'^2 \equiv_{p^{\alpha-1}} a. \tag{32.19}$$

To determine the last digit $x_{\alpha-1} \in \{0, 1, \ldots, p-1\}$ of $x = x' + x_{\alpha-1} p^{\alpha-1}$, write $x'^2 = a + bp^{\alpha-1}$ for some integer b, and then work modulo p^α as follows:

$$x^2 = (x' + x_{\alpha-1} p^{\alpha-1})^2 \equiv_{p^\alpha} x'^2 + 2x_0 x_{\alpha-1} p^{\alpha-1} \tag{32.20}$$

$$= a + p^{\alpha-1}(b + 2x_0 x_{\alpha-1}). \tag{32.21}$$

So it suffices to choose

$$X_{\alpha-1} \equiv_p -(2x_0)^{-1} b \tag{32.22}$$

Claim 32.3 $2x_0$ *is invertible.*

Proof: Since p is odd, and $a \equiv_p x_0^2$ is prime to p. □ □

32.4 Example 4

Example 32.4 *Prove that*

$$\prod_{\textit{all primes } p} \frac{1}{1 - \frac{1}{p}} \tag{32.23}$$

diverges to infinity. Using this prove that the sum of the reciprocals of the primes diverges.

Proof: Expand each term in the product in a geometric series:

$$(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots). \tag{32.24}$$

In expanding all the parentheses, the denominators will be all possible expressions of the form

$$p_1^{\alpha_1} \ldots p_r^{\alpha_r}. \tag{32.25}$$

According to the Fundamental Theorem, every positive integer n occurs exactly once as such an expression. Hence the product is equal to the harmonic series

$$\sum_{n=1}^{\infty} \frac{1}{n} \tag{32.26}$$

which we know diverges.

For the second part, we first note that for $x \leq \frac{1}{2}$, we have

$$x \geq -\frac{1}{2}\log(1-x). \tag{32.27}$$

When $x = \frac{1}{p}$ for prime p, the previous result holds. Now take the log of the product in the previous part:

$$\log(\prod_{\text{all primes } p} \frac{1}{1-\frac{1}{p}}) = \sum_{\text{all primes } p} -\log(1-\frac{1}{p}). \tag{32.28}$$

By the result in equation 32.27 the RHS is less than

$$2 \sum_{\text{all primes } p} \frac{1}{p} \tag{32.29}$$

which is the sum of the reciprocals of the primes. Since we know that the product in 32.23 diverges, the sum of the reciprocals of the primes also diverges. □

32.5 Example 5

Example 32.5 *Suppose that m is either a power p^α of a prime $p \geq 2$ or else twice an odd prime power. Prove that, if $x^2 \equiv_m 1$, then either $x \equiv_m 1$ or $x \equiv_m -1$. Also this is always false if m is not of the form p^α or $p^{2\alpha}$, and $m \neq 4$.*

Proof: Suppose that $m = 2p^\alpha$. Since $m|(x^2-1) = (x+1)(x-1)$, we must have α powers of p appearing in both $x+1$ and $x-1$ together. But since $p \geq 3$, it follows that p cannot divide both $x+1$ and $x-1$ (since they are only two apart from one another). Thus all the of the p's must divide one of them. If $p^\alpha|x+1$, this means that $x \equiv_{p^\alpha} -1$; if $p^\alpha|x-1$, then $x \equiv_{p^\alpha} 1$. Finally, since $2|x^2-1$ it follows that x must be odd, i.e., $x \equiv_2 1$. Thus, either $x \equiv_{2p^\alpha} 1$ or $x \equiv_{2p^\alpha} -1$. The proof for the case $m = p^\alpha$ is the first part of the earlier proof.

First, if $m \geq 8$ is a power of 2, it's easy to show that $x = \frac{m}{2}+1$ gives a contradiction to the earlier part.

Next suppose that m is not a prime power (or twice a prime power), and

$$p^\alpha \| m. \tag{32.30}$$

Set

$$m' = \frac{m}{p^\alpha}. \tag{32.31}$$

We can use the Chinese Remainder theorem to find an x which is $\equiv_{p^\alpha} 1$ and $\equiv_{m'} -1$.

Let $x = rp^\alpha + 1$ and $x = sm' - 1$. Consider

$$\begin{aligned} x^2 &= (rp^\alpha+1)(sm'-1) && (32.32)\\ &= rs\dot{m} - (rp^\alpha+1) + 1 + (sm'-1) + 1 - 1. && (32.33)\end{aligned}$$

Hence $x^2 \equiv_m 1$. But $x \equiv_m 0$ by the Chinese Remainder Theorem. This contradicts the first part. □

Chapter 33

Vipul Jain

33.1 Primes and their Distribution

Theorem 33.1 *1. Prove that if $n > 2$, then there exists a prime p satisfying $n < p < n!$.*

2. For $n > 1$, show that every prime divisor of $n! + 1$ is an odd integer greater than n.

Proof:

1. Consider (n! - 1). Let p be a prime factor of (n! - 1). If (n! -1) is a prime, p = (n! - 1). If (n! - 1) is composite, then a $\nmid$ (n! - 1) $\forall$ positive integer 2 $\leq$a $\leq$ n since a | n! but a $\nmid$ 1. So p ¿ n. Since (n! - 1) is composite, p < n!. Hence prime number p satisfies n < p < n!.
2. If n = 1, then n! + 1 = 2 which is even and has 2 as a prime factor. If n > 1, then n! is even as 2 is a factor of n!. This means that (n! + 1) is odd $\forall$ n > 1. So all prime factors of n are odd. Let p be a prime factor of (n! + 1). We note that $\forall$ 1 < a $\leq$ n, (n! + 1) $\equiv_a$ = 1. $\therefore$ all prime factors of (n! + 1) are greater than n and this completes the proof.

□

33.2 Linear Congruence

Exercise 33.1 *(Ancient Chinese Problem) A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal proportions, 3 coins remained. In the ensuing brawl over who should get the extra coins, one pirate was killed. The wealth was redistributed, but this time an equal division left 10 coins. Again an argument developed in which another pirate was killed. But now, the total fortune was evenly distributed among the survivors. What was the least number of coins that could have been stolen?*

Solution: Let the number of coins stolen was x. We form Linear congruences from given data.

$$x = 3 \pmod{17} \quad (33.1)$$
$$x = 10 \pmod{16} \quad (33.2)$$
$$x = 0 \pmod{15} \quad (33.3)$$

17*16*15 = 4080. $\therefore$ we need to find x (mod 4080) that satisfies all three congruences (From Chinese Remainder theorem). Since $r_3 = 0$, we only need todetermine N_i and x_i for i = 1 and 2.
$r_1 = 3$, N_1 = 16*15 = 240
Solving $240x_1 \equiv_{17} 1$ gives $x_1 = 9$ as solution.
$r_2 = 10$, N_2 = 17*15 = 255
Solving $255x_2 \equiv_{16} 1$ gives x_2 = -1 as solution.
Thus, x = 3*240*9 + 10*255*(-1) = 3930 (mod 4080) are the solutions. Since we want smallest positive solution, x = 3930 is the solution. Hence the least number of coins that could have been stolen is 3930.

□

33.3 The Fibonacci Sequence

Theorem 33.2 *Show that the sum of the squares of the first n Fibonacci numbers is given by the formula*

$$u_1^2 + u_2^2 + u_3^2 + \cdots + u_n^2 = u_n u_{n+1} \tag{33.4}$$

Proof:

$$u_{n+1} = u_n + u_{n-1} \tag{33.5}$$
$$\Rightarrow u_n = u_{n+1} - u_{n-1} \tag{33.6}$$
$$u_1^2 = u_1 u_2 \text{ (} as\ u_1 = u_2 = 1 \text{)} \tag{33.7}$$

$\forall n \geq 2$ (u_{n-1} is defined only if n $\geq$ 2)

$$u_n^2 = u_n.u_n = u_n.(u_n + u_{n-1}) \text{ (} from(33.6) \text{)} \tag{33.8}$$
$$\Rightarrow u_n^2 = u_n.u_{n+1} - u_n.u_{n-1} \tag{33.9}$$

Now consider $u_1^2 + u_2^2 + u_3^2 + \cdots + u_n^2$.

$$\begin{aligned} u_1^2 + u_2^2 + u_3^2 + \cdots + u_{n-1}^2 + u_n^2 &= u_1u_2 + (u_2u_3 - u_2u_1) + (u_3u_4 - u_3u_2) + \ldots \\ &\quad +(u_{n-1}u_n - u_{n-1}u_{n-2}) + (u_nu_{n+1} - u_nu_{n-1}) \quad (33.10) \\ &= u_nu_{n+1} \text{ (} As\ all\ other\ terms\ cancel\ out \text{)} \quad (33.11) \end{aligned}$$

□

33.4 Euler's Phi function

Theorem 33.3 *Prove that the equation $\phi(n) = \phi(n + 2)$ is satisfied by n = 2(2n - 1) whenever p and 2p - 1 are both odd primes.*

Proof: First, note that for integers m and n such that gcd(m,n) = 1, $\phi(mn) = \phi(m)\phi(n)$ because ϕ is a multiplicative function.

If 2p-1 is prime, then

$$\phi(n) = \phi(2(2p-1)) = \phi(2(2p-1) = \phi(2)\phi(2p-1) = 1.((2p-1)-1) = 2p-2 \tag{33.12}$$

Now, n + 2 = 2(2p - 1) + 2 = 4p. Since p is odd, we have

$$\phi(n + 2) = \phi(4p) = \phi(4)\phi(p) = 2(p-1) = 2p-2 \tag{33.13}$$

$\therefore \phi(n) = \phi(n + 2)$ if n = 2(2p - 1) where both p and (2p - 1) are primes. □

33.5 Fermat's Little Theorem

Theorem 33.4 *Prove that if p is an odd prime and k is an integer satisfying* $1 \leq k \leq$ *(p-1), then the binomial coefficient* $\left(\begin{array}{c} p-1 \\ k \end{array} \right) \equiv_p (-1)^k$.

Proof:

$$\begin{aligned}
\left(\begin{array}{c} p-1 \\ k \end{array} \right) &= \frac{(p-1)!}{(p-1-k)!k!} && (33.14)\\
&= \frac{(p-1)(p-2)\dots(p-k)}{k!} && (33.15)\\
&= \frac{p\{(p-2)(p-3)\dots(p-k))\}}{k!} + \frac{(-1)^1 1!\{(p-2)(p-3)\dots(p-k))\}}{k!} && (33.16)\\
&= \frac{p\{(p-2)(p-3)\dots(p-k))\}}{k!} + \frac{(-1)^1 1!p\{(p-3)(p-4)\dots(p-k))\}}{k!} \\
&\quad + \frac{(-1)^2 2!\{(p-3)(p-4)\dots(p-k))\}}{k!} && (33.17)\\
&= \vdots && (33.18)\\
&= \frac{p\{(p-2)(p-3)\dots(p-k))\}}{k!} + \frac{(-1)^1 1!p\{(p-3)(p-4)\dots(p-k))\}}{k!} \\
&\quad + \dots + \frac{(-1)^{k-1}(k-1)!p^{k-1}(p-k)}{k!} + \frac{(-1)^{k-1}(k-1)!p^k}{k!} + \frac{(-1)^k k!}{k!} && (33.19)\\
&= \frac{p\{(p-2)(p-3)\dots(p-k))\}}{k!} + \frac{(-1)^1 1!p\{(p-3)(p-4)\dots(p-k))\}}{k!} \\
&\quad + \dots + \frac{(-1)^{k-1}(k-1)!p^{k-1}(p-k)}{k!} + \frac{(-1)^{k-1}(k-1)!p^k}{k!} + (-1)^k && (33.20)
\end{aligned}$$

Now, from (33.20), we conclude that $\frac{p\{(p-2)(p-3)\dots(p-k))\}}{k!} + \frac{(-1)^1 1!p\{(p-3)(p-4)\dots(p-k))\}}{k!} + \dots + \frac{(-1)^{k-1}(k-1)!p^{k-1}(p-k)}{k!}$ $+ \frac{(-1)^{k-1}(k-1)!p^k}{k!}$ is an integer as $(-1)^k$ is an integer and left hand side of equation is also an integer. Also, p is prime and k < p, hence gcd(p,k!) = 1. Since we can take out p common from $\frac{p\{(p-2)(p-3)\dots(p-k))\}}{k!} + \frac{(-1)^1 1!p\{(p-3)(p-4)\dots(p-k))\}}{k!} + \dots + \frac{(-1)^{k-1}(k-1)!p^{k-1}(p-k)}{k!} + \frac{(-1)^{k-1}(k-1)!p^k}{k!}$, it is divisible by p. Hence we get

$$\begin{aligned}
\frac{p\{(p-2)(p-3)\dots(p-k))\}}{k!} + \frac{(-1)^1 1!p\{(p-3)(p-4)\dots(p-k))\}}{k!} &\equiv_p 0 \\
+ \dots + \frac{(-1)^{k-1}(k-1)!p^{k-1}(p-k)}{k!} + \frac{(-1)^{k-1}(k-1)!p^k}{k!} & && (33.21)
\end{aligned}$$

From (33.20) and (33.21), we get

$$\left(\begin{array}{c} p-1 \\ k \end{array} \right) \equiv_p (-1)^k \qquad (33.22)$$

This completes the proof. □

Chapter 34

Tushar Chaudhary

34.1 Fibonacci numbers

Exercise 34.1 *Show that F(n) is a multiple of 3 iff* $4|n$

Solution ($\Longrightarrow$)

$$\begin{aligned} F(n+4) &= F(n+3) + F(n+2) \\ &= 2 * F(n+2) + F(n+1) \\ &= 3 * F(n+1) + F(n) \end{aligned}$$

This proves that if F(n) is a multiple of 3, F(n+4) is also a multiple of 3. Since F(0) is 0(3*0), it goes on to say that every fourth Fibonacci number is a multiple of 3. Hence if $4|n$, F(n) is a multiple of 3.

($\Longleftarrow$)
We know that gcd(F(n),F(n+1)) = 1.
So since $3|F(n), F(n+1)$ can not be a multiple of 3. Similarly since $3|F(n+4)$, F(n+3) can not be a multiple of 3.
F(n+2) = F(n+1) + F(n)
Since $3|F(n)$ and F(n+1) is not a multiple of 3, F(n+2) can not be a multiple of 3.
Hence proved.

34.2 Chinese Remainder Theorem

Exercise 34.2 *Under the definitions of Chinese Remainder Theorem, prove that the number of roots of the equation f(x) ≡ 0 (mod n) is equal to the product of the number of roots of each of the equations f(x) ≡ 0 (mod* n_1*),f(x) ≡ 0 (mod* n_2*),...,f(x) ≡ 0 (mod* n_k*).*

Solution By Corollary 33.22 in "Introduction to Algorithms - Cormen, Leiserson, Rivest", we know that the equation

$$ax \equiv b(modn)$$

has d distinct solutions, where $d = gcd(a, n)$ or no solutions. The equation has d distinct solutions in the case when gcd(a,n) | b. Without the loss of generality, lets assume f(x) = ax - b.
Case 1 When the system has d distinct solutions.

In this case, gcd(a,n) | b. Number of solutions will be equal to gcd(a,n). Since all n_i are factors of n, they all divide b. hence each of the k equations will have $gcd(a, n_i)$ solutions.
It remains to prove that

$$gcd(a, n) = \prod_{1}^{k} gcd(a, n_i)$$

The above result follows from the fact that all n_is are pairwise relatively prime.
Case 2 When the system has no solutions.
In this case, gcd(a,n) does not divide b.
Then $gcd(gcd(a, n), b) = k \neq gcd(a, n)$. Hence gcd(a,n) = kk' where k' and b are relatively prime. Since all n_i are pairwise relatively prime, atleast one n_i divides k' and hence does not divide b. The equation corresponding to that n_i will have no roots. Hence proved.

34.3 Wilson's Theorem

Exercise 34.3 *Wilson's Theorem states that if p is a prime, then $(p-1)! \equiv -1(modp)$. Prove that the converse is also true if $p \geq 2$: in other words, show that if p is an integer, $p \geq 2and(p-1)! \equiv -1(modp)$ then p is prime.*

Solution Suppose that $(p-1)! \equiv -1(modp)$ and that $1 \leq a \leq p-1$ is a divisor of p. Thus

$$a|(p-1)!$$

but also

$$(p-1)! \equiv -1(moda)$$

$$\Rightarrow a|(p-1)! + 1$$

$$\Rightarrow a|1$$

hence a must be 1.
So the only positive divisors of p are p and 1. Hence, if $p \geq 2$, p is a prime.

Hence proved.

34.4 GCD, Continued Fractions

Exercise 34.4 *In the Euclidean algorithm for finding gcd(a, b), we use repeated division with quotient and remainder*

$$a = q_0 b + r_0$$

$$b = q_1 r_0 + r_1$$

$$r_0 = q_2 r_1 + r_2$$

$$....,$$

$$r_{k-2} = q_k r_{k-1} + 0$$

Prove that the continued fraction for $\frac{a}{b}$ is $[q_0 : q_1, q_2, ..., q_k]$.

Solution We prove by induction on k, the number of non-zero remainders got in the Euclidean algorithm. As base case we consider k=0,1.

For k=0, $a = q_0 b$. The continued fraction for $\frac{a}{b}$ in this case is simply $[q_0]$.

For k=1, $a = q_0 b + r_0; b = q_1 r_0 + 0$. The computation for the continued fraction in this case gives

$$\begin{aligned} \frac{a}{b} &= q_0 + \frac{r_0}{b} \\ &= q_0 + \frac{1}{\frac{b}{r_0}} \\ &= q_0 + \frac{1}{q_1} \\ &= [q_0 : q_1] \end{aligned}$$

Propogation Step : If the result is true for the Euclidean Algorithm with k non-zero remainders and for continued fractions with k terms, then the result holds for k+1 as well.

For the k+1 case, we have $a = q_0 b + r_0; b = q_1 r_0 + r_1; r_1 = q_2 r_1 + r_2; .....; r_{k-1} = q_{k+1} r_k + 0$
Now we know that for b, r_0, the continued fraction is

$$q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{....}}}$$

Then $\frac{a}{b} = q_0 + \frac{r_0}{b}$

$$\frac{a}{b} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{....}}}}$$

i.e $[q_0 : q_1, q_2, ..., q_{k+1}]$

Hence Proved

34.5 Fermat's Little Theorem

> *I confess that Fermat's Theorem as an isolated proposition has very little interest for me, because I could easily lay down a multitude of such propositions, which one could neither prove nor dispose of.*
> –Karl Friedrich Gauss (1777-1855)

Exercise 34.5 (a) *Suppose a is a quadratic residue modulo some prime $p > 2$. Prove that a is not a primitive*
(b) *Let p be a prime. What is the value of $\sum_{a=1}^{p-1} a^p$ mod p root mod p.*

Solution (a) Assume $a \equiv x^2$ mod p; Raising both sides to the power $\frac{p-1}{2}$ we get

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 mod p$$

by Fermat's Little Theorem.

Thus a has at most order $\frac{p-1}{2}$ which implies that a cannot be a primitive root mod p since primitive roots have order p-1.

Solution (b) By Fermat's Little Theorem we have,

$$\begin{aligned} a^{p-1} &\equiv 1 mod p \\ \Rightarrow a^p &\equiv a mod p \\ \Rightarrow S := \sum_{a=1}^{p-1} a^p &\equiv \sum_{a=1}^{p-1} a \\ &= \frac{p(p-1)}{2} mod p \end{aligned}$$

If $p = 2$ then $S \equiv 1 mod 2$.
If $p > 2$, then $S \equiv 0 mod p$ since $p|p(p-1)$ but does not divide 2.

Chapter 35

Keshav Kunal

35.1 Infinitude of Primes

Exercise 35.1 *Use Bertrand's Postulate to show that:*

1. *If $n > 6$, then n can be expressed as the sum of distinct primes.*
2. *The equation*
$$\frac{1}{n} + \frac{1}{n+1} \cdots + \frac{1}{n+k} = m$$
does not admit positive integer solutions.
3. *The equation*
$$n! = m^k$$
has integer solutions if at least one of k, n or m is 1.

Solution: Bertrand's Postulate states that if $n > 0$, then there is a prime p satisfying $n < p \leq 2n$.

1. Proof by Induction:
Base: $7 = 5 + 2$
I.H.:Assume true for all $k, 6 < k \leq n$.
If $n+1$ is a prime, we are done. Assume $n+1$ is not a prime. Using the postulate, there exists a prime p, $\frac{n+1}{/}2 < p < n$. Using the *I.H.*, $n+1-p$ can be expressed as sum of distinct primes,say $p_1 + p_2 \ldots + p_j$. Also, $p > n+1-p$ and hence $n+1 = p_1 + p_2 \ldots + p_j + p$ where each prime is distinct.

2. *Case 1:* $1 \leq k < n$.
$$\frac{1}{n} + \frac{1}{n+1} + \cdots + \frac{1}{n+k} < \frac{1}{n} + \frac{1}{n+1} \cdots + \frac{1}{2n} \leq 1$$
So, $m < 1$ and there is no integer solution.
Case 2: $1 \leq n \leq k$.
Consider the biggest prime $p, n < p \leq n+k$. Such a prime exists by Bertrand's postulate.
$$\frac{1}{n} + \frac{1}{n+1} \cdots + \frac{1}{n+k} = \frac{\Sigma_{i=0}^{k} \Pi_{j \neq i}(n+j)}{\Pi_j n + j}$$
In the numerator, p divides all terms except the one corresponding to $i = p - n$. Also, p divides the denominator. Hence the denominator does not divide the numerator and the value is not integral.

3. Consider the prime factors of $n!$. If $n! = m^k$ for $k \geq 2$, every prime factor should occur atleast twice in the prime factorization of $n!$. Now, consider the largest prime p such that $n/2 < p \leq n$. Clearly $p|n!$ but $p^2 \not| n!$ as p is the only number between 1 and n which divides p. So, there exist no solutions for $k > 1$.

   Trivial solutions can be constructed when either of n, k or m is 1.

□

35.2 Quadratic Residues

Exercise 35.2 *Show that very positive integer can be expressed as the sum of four squares.*

Solution:

Claim 35.1 *If two integers can be expressed as the sum of four squares, so can their product.*

Proof. Assume $n_1 = a^2 + b^2 + c^2 + d^2$ and $n_2 = x^2 + y^2 + z^2 + t^2$. Note that n_1 can be expressed as $\alpha\bar{\alpha}$, where $\alpha = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$. Similarly, $n_2 = \beta\bar{\beta}$, where $\beta = x + y\boldsymbol{i} + z\boldsymbol{j} + t\boldsymbol{k}$. Now,

$$(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + t^2) = \alpha\bar{\alpha}\beta\bar{\beta}$$

$\beta\bar{\beta}$ is real and so commutes with $\bar{\alpha}$. Thus,

$$\begin{aligned} n_1n_2 = \alpha\bar{\alpha}\beta\bar{\beta} &= \alpha\beta\bar{\beta}\bar{\alpha} \\ &= \alpha\beta\overline{\alpha\beta} \\ &= (ax - by - cz - dt)^2 + (ay + bx + ct - dz)^2 + (az - bt + cx + dy)^2 + (at + bz - cy + dx)^2 \end{aligned} \tag{35.1}$$

Hence the product can be expressed as the sum of four squares.
The next two claims will show that any prime number can be expressed as the sum of four squares.

Claim 35.2 *There exist integers a, b, c, d such that $a^2 + b^2 + c^2 + d^2 = mp$, where $m < p$.*

There are $\frac{1}{2}(p-1)$ quadratic residues in $\mathbb{Z}_p$. Since 0 is also a square,$\mathbb{Z}_p$ contains $\frac{1}{2}(p+1)$ squares. The two sets $\{x^2 + 1 | x \in \mathbb{Z}_p\}$ and $\{-x^2 | x \in \mathbb{Z}_p\}$ contain $\frac{1}{2}(p+1)$ elements each in $\mathbb{Z}_p$. Now, $2 \cdot \frac{1}{2}(p+1) = p + 1 >$ number of distinct elements in $\mathbb{Z}_p$. So, there exist integers such that $x^2 + y^2 + 1 \equiv_p 0$. $x^2 \equiv_p (p-x)^2$, so if $0 \leq x < p$, either x or $p - x < \frac{p}{2}$. There exist integers x, y with $0 \leq x, y < \frac{p}{2}$ such that

$$x^2 + y^2 + 1^2 + 0^2 \equiv_p 0 \Rightarrow x^2 + y^2 + 1^2 + 0^2 = mp$$

Now $x^2, y^2 < (\frac{p}{2})^2$. Hence $x^2 + y^2 + 1^2 + 0^2 < \frac{p^2}{2} + 1 < p^2$ for $p > 2$. So the factor m in 35.2 is less than p which completes the proof of the claim.

Claim 35.3 *Any odd prime p can be expressed as the sum of four squares.*

From the previous claim we have,

$$a^2 + b^2 + c^2 + d^2 = mp, \quad \text{where} m < p$$

case: m is even
a, b, c, d can be divided into two pairs such that a pair contains both even or both odd numbers. *wlog* assume (a, b) and (c, d) form such pairs. Using

$$(\frac{a+b}{2})^2 + (\frac{a-b}{2})^2 + (\frac{c+d}{2})^2 + (\frac{c-d}{2})^2 = \frac{1}{2}(a^2 + b^2 + c^2 + d^2)$$

we can find a $m' < m$ such that $m'p$ can be expressed as the sum of four squares.
case: m is odd
Choose numerically least x, y, z, t such that $x \equiv_m a, y \equiv_m b, z \equiv_m c$ and $t \equiv_m d$. It is easy to see that

$$a^2+b^2+c^2+d^2 \equiv_m 0x^2+y^2+z^2+t^2 \equiv_m 0ax+by+cz+dt \equiv_m 0ay-bx-ct+dz \equiv_m 0az+bt-cx-dy \equiv_m 0at-bz+cy-dx \equiv_m 0$$

Using $\alpha = a - b\boldsymbol{i} - c\boldsymbol{j} - d\boldsymbol{k}$ and the proof of 35.1, we get

$$(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2) = (ax+by+cz+dt)^2+(ay-bx-ct+dz)^2+(az+bt-cx-dy)^2+(at-bz+cy-dx)^2$$

Since numerically least values have been chosen, $x, y, z, t < \frac{m}{2}$ and hence

$$x^2 + y^2 + z^2 + t^2 = m'm < \left(\frac{m}{2}\right)^2 \cdot 4 = m^2$$

Dividing the equation 35.2 by m^2 gives $m'p$, where$m' < m$ as the sum of four squares.
We have shown that for an odd prime p,we can progressively choose smaller values of m such that mp can be expressed as sum of four squares. Hence following this method of descent, we can finally express p as the sum of four squares.

Since every number has a unique prime factorization, using the previous claim we can express each prime(note that $2 = 0^2 + 0^2 + 1^2 + 1^2$) as a sum of four squares and then use claim35.1 repeatedly to get four squares which sum up to the number. □

35.3 Approximation of Irrationals

Exercise 35.3 *Show that for an irrational number α, the convergent $\frac{p_n}{q_n}$ is the best approximation to α relative to any y satisfying*

1. *$y < q_{n+1}$ if $a_{n+1} = 1$*
2. *$y < q_{n-1} + a_{n+1}q_n/2$ if $a_{n+1} > 1$*

Hence show that 22/7 is the best approximation to π relative to any integer less than 54. *Solution:* We shall consider case (ii) when n is even. Choose $\beta = 2\alpha - p_n/q_n$ which implies $\alpha - \frac{p_n}{q_n} = \beta - \alpha$. So, we have

$$\frac{p_n}{q_n} < \alpha < \frac{p_{n+1}}{q_{n+1}} < \beta < \frac{p_{n-1}}{q_{n-1}}$$

Consider the interval I $(\frac{p_n}{q_n}, \delta)$ where δ lies midway between $\frac{p_{n+1}}{q_{n+1}}$ and $\frac{p_{n-1}}{q_{n-1}}$. We claim that it contains the interval $(\frac{p_n}{q_n}, \beta)$ by proving the following claim
Claim: $\beta < \delta$
Proof. A rational number lying strictly between $\frac{p_n}{q_n}$ and $\frac{p_{n-1}}{q_{n-1}}$ has the form

$$T(s,t) = \frac{sp_{n-1} + tp_n}{sq_{n-1} + tq_n}$$

Note that $\delta = T(2, a_{n+1}) = T(1, a_{n+1}/2)$. We will show that $\beta < T(1, \theta)$ for $\theta \leq a_{n+1}/2$.

$$\beta < T(1,\theta) \iff 2\alpha - \frac{p_n}{q_n} < \frac{p_{n-1}}{q_{n-1}} - \frac{\theta}{q_{n-1}(q_{n-1}+\theta q_n)}$$

But we know that,

$$\frac{p_{n-1}}{q_{n-1}} = \frac{p_n}{q_n} + \frac{1}{q_n q_{n-1}} \qquad \text{and} \qquad \alpha - \frac{p_n}{q_n} < \frac{1}{q_n q_{n+1}}$$

Using the above results we get,

$$\begin{aligned} \frac{2}{q_n q_{n+1}} &< \frac{1}{q_n q_{n-1}} - \frac{\theta}{q_{n-1}(q_{n-1}+\theta q_n)} \\ &= \frac{1}{q_n(q_{n-1}+\theta q_n)} \\ \Rightarrow q_n(q_{n-1}+2\theta q_n) &< a_{n+1} q_n \\ \Rightarrow \frac{q_{n-1}}{2q_n} + \theta &< \frac{a_{n+1}}{2} \end{aligned}$$

Hence as $q_{n-1} < q_n$, the equation (35.3) holds if $\theta \leq q_{n+1}/2$ which completes the proof of the claim.
Now suppose u/v is a rational number in interval I. As the length of this interval is greater than $u/v - \frac{p_n}{q_n}$,

$$0 < \frac{uq_n - vp_n}{q_n v} < \frac{1}{q_n(q_{n-1}+a_{n+1}q_n/2)}$$

The numerators and denominators of these fractions are integers and hence we get $v > q_{n-1} + a_{n+1}q_n/2$. This implies that no rational number in the interval I has a denominator less than $q_{n-1} + a_{n+1}q_n/2$ which implies $\frac{p_n}{q_n}$ is the best approximation.

Note that the SICF representation of $\pi = [3, 7, 15\ldots]$. Using the theorem 22/7 is the best approximation to π relative to any integer less than $1 + 15.7/2 = 53\frac{1}{2}$. □

35.4 Congruences

Exercise 35.4 *Show that the equation*

$$(7a+1)x^3 + (7b+2)y^3 + (7c+4)z^3 + (7d+1)xyz = 0$$

has no non-trivial solutions

Solution: We will show that the equation

$$(7a+1)x^3 + (7b+2)y^3 + (7c+4)z^3 + (7d+1)xyz \equiv_7 0$$

$$\iff (x^3 + 2y^3 + 4z^3 + xyz \equiv_7 0$$

has no non-trivial solution which proves the result because any non-trivial solution to eqn.(35.4) will also be a non-trivial solution to it. We will use the following claim,
Claim:$x^3 \equiv_7 0, +1, -1$
This claim can be proved by considering all possible values of x modulo 7.

Consider the following cases for eqn.(35.4).
Case: $z \equiv_7 0$. The equation reduces to $x^3 + 2y^3 \equiv_7 0$ which does not have a non-trivial solution.
Case:$z \not\equiv_7 0$. The equation reduces to $x^3 + 2y^3 \pm 4 \pm xy \equiv_7 0$. Consider the following sub cases.

1. $x \equiv_7 0$. The equation reduces to $2y^3 \pm 4 \equiv_7 0$, which does not have a solution.
2. $y \equiv_7 0$. The equation reduces to $x^3 \pm 4 \equiv_7 0$, which does not have a solution.
3. $x \equiv_7 \pm 1, y \equiv_7 \pm 1$. The equation reduces to $\pm 1 \pm 2 \pm 4 \pm 1 \equiv_7 0$, which does not have a solution.

□

35.5 Divisibility

Exercise 35.5 *The Farey series F_n of order n is the increasing sequence of all irreducible fractions lying between 0 and 1 whose denominators do not exceed n, so $0 \leq a \leq b \leq n$ and $(a,b) = 1$. For instance the Farey series of order 4 is $0/1, 1/4.1/3, 1/2, 2/3 \ldots$. Assume that a/b,c/d,e/f are consecutive terms in the series F_n. Show that:*

1. $bc - ad = 1$
2. $c/d = (a+e)/(b+f)$
3. *Use the above parts to find the two terms which succeed $3/7$ in F_{11}*

Solution:

1. The general solutions of $bx - ay = 1$ are given by

$$x = x_0 + ta \quad , \quad y = y_0 + tb$$

Choose t such that $n - b < y \leq n$. So $x/y \in F_n$ and $x/y \geq c/d$. We will show $x/y = c/d$ by contradiction. Assume $x/y > c/d$.So,we have

$$\begin{aligned} x/y - a/b &\geq 1/dy \\ c/d - a/b &\geq 1/bd \end{aligned}$$

Also,

$$\begin{aligned} 1/by &= (bx - ay)/by \\ &= x/y - a/b \\ &\geq 1/dy + 1/bd \\ &= (b+y)/bdy \\ &> n/bdy \\ &\geq 1/by \end{aligned}$$

which is a contradiction.

2. From the previous part we know that,

$$\begin{aligned} bc - ad &= 1 \\ de - cf &= 1 \end{aligned}$$

Solving for c and d, we get $c = \frac{a+e}{be-af}$ and $d = \frac{b+f}{be-af}$.Hence we get the result.

3. The next two terms are $4/9$ and $5/11$.

□

Chapter 36

Akrosh Gandhi

36.1 Euclidean Algorithm

Exercise 36.1 *Prove that if $m \geq n$, then $a^{2^n}+1$ devides $a^{2^m}-1$. Also show that a, m, n are positive integer with $m \geq n$, Then*

$$gcd(a^{2^m}+1, a^{2^n}+1) = \begin{cases} 1 & \text{if } a \text{ is even} \\ 2 & \text{if } a \text{ is odd} \end{cases}$$

Proof: As we have given $m > n$ let $a \geq 1$, then we can say that $m \geq n+1$ and $(a^{2^n+1}-1) = (a^{2^n}+1)(a^{2^n}-1)$ so that $(a^{2^n}+1)|(a^{2^n+1}-1)$. since $m \geq n+1$, $a^{2^n+1}-1$ devides $a^{2^m}-1$ because $2^{n+1}|2^m$. so concludingly we can say $(a^{2^n}+1)|(a^{2^m}-1)$.
let $d = gcd(a^{2^m}+1, a^{2^n}+1)$ then $d|a^{2^m}+1$ and $d|a^{2^m}+1$. From previous result $(a^{2^n}+1)|(a^{2^m}-1)$ so $d|a^{2^m}-1$, Hence $d|(a^{2^m}+1)-(a^{2^m}-1)$, this implies $d|2$. d is 1 or 2 and hence $gcd(a^{2^m}+1, a^{2^n}+1)$ is 1 or 2.
if a is even then $a^{2m}+1$ is odd so that $gcd(a^{2^m}+1, a^{2^n}+1) = 1$
if a is odd then $a^{2^m}+1$ is even so that $gcd(a^{2^m}+1, a^{2^n}+1) = 2$

□

36.2 Linear Conrguence

Exercise 36.2 *Let p be an odd prime and $r > 1$. Show that there are exactly two solution (mod p^r) to the congruence $x^2 \equiv 1(mod p^r)$. More generally, show that if $gcd(a, p^r) = 1$ then congruence $x^2 \equiv a(mod p^r)$ either has no solution or has two solution mod p^r.*

Proof: if $x^2 \equiv 1(modp^r)$ then $x^2 - 1 \equiv 0(modp^r)$ so $p|(x-1)(x+1)$. Since $p|p^r$ and p is prime, it follows that either $p|(x-1)$ or $p|(x+1)$ (or both). However if it divides both factor then p divides $2 = (x+1)-(x-1)$, which is impossible, since p is an odd prime. Hence p divides exactaly one of $x \pm 1$.
if $p|(x-1)$ then $gcd(x+1, p^r) = 1$, so from $p^r|(x-1)(x+1)$ we deduce that $p^r|(x-1)$, that is, $x \equiv 1(modp^r)$. Similarly, if $p|(x+1)$ then $x \equiv -1(modp^r)$. Hence the congruence $x^2 \equiv 1(modp^r)$ has two solution mod p^r, namely $x \equiv \pm 1(modp^r)$.
More generally, if $gcd(a, p^r) = 1$ and $x^2 \equiv a(modp^r)$ then $gcd(a, p) = 1$. We need to show that if $x^2 \equiv y^2(modp^r)$ with $gcd(a, p) = 1$ then $y \equiv \pm x(modp^r)$. As before, we have $p^r|(x-y)(x+y)$, so either $p|(x-y)$ or $p|(x+y)$. These cannot both occur, since otherwise p divides $(x+y)+(x-y) = 2x$, which is impossible. Hence either $gcd(x+y, p^r) = 1$ or $gcd(x-y, p^r) = 1$ and therefore $x \equiv y(modp^r)$ or $x \equiv -y(modp^r)$. □

36.3 Periodic Continued Fraction

Exercise 36.3 *Let N be a positive integer(not square). Let p_j and q_j are defined as notes. From continued fraction of $\sqrt{N}$, let S_n is defined as in $\frac{m_n+\sqrt{N}}{S_n}$. Then proove for every non negative integer n we have $p_{n-1}^2 - Nq_{n-1}^2 = (-1)^n S_n$.*

Proof: As we know earlier that quadratic irrational $\alpha = \frac{m_0+\sqrt{N}}{S_0}$.Let put $m_0 = 0$ and $S_0 = 1$ then we have $\alpha = \sqrt{N}$. p_j and q_j are defined as $p_j = p_{j-1}a_j + p_{j-2}$ and $q_j = q_{j-1}a_j + q_{j-2}$.
Write $\sqrt{N} = [a_0, a_1, \ldots, a_{n-1}, a_n]$ This is periodic continued fraction so

$$\sqrt{N} = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} = \frac{(m_n + \sqrt{N})p_{n-1} + S_n p_{n-2}}{(m_n + \sqrt{N})q_{n-1} + S_n q_{n-2}} \tag{36.1}$$

Which implies

$$Nq_{n-1} + (m_n q_{n-1} + S_n q_{n-2})\sqrt{N} = (m_n p_{n-1} + S_n p_{n-2}) + p_{n-1}N \tag{36.2}$$

Since $\sqrt{N}$ is irrational,

$$m_n q_{n-1} + S_n q_{n-2} = p_{n-1} \text{ and } m_n p_{n-1} + S_n p_{n-2} = Nq_{n-1}$$

By apply simple mathematics ,

$$p_{n-1}^2 - Nq_{n-1}^2 = S_n(p_{n-1}q_{n-2} - p_{n-2}q_{n-1}) \tag{36.3}$$

As follows from notes that $p_{n-1}q_{n-2} - p_{n-2}q_{n-1} = (-1)^n$ we proved that
$p_{n-1}^2 - Nq_{n-1}^2 = (-1)^n S_n$ Hence proved.

□

36.4 Quadratic Reciprocity

Exercise 36.4 *If p is a prime and $p = x^2 + ny^2$, where x, y, nZ, prove that $gcd(x, y) = 1$ and* $\left[\begin{array}{c} -n \\ p \end{array}\right] = 1$.

Proof: Let say $d = gcd(x, y)$, then d is divisor of both x and y, so $d|x$ and $d|y$, but we have $p = x^2 + ny^2$ so $d|p$, but p is prime hence d is either 1 or p. if d is p then $p|x$,but that is not possible,because it contradict $p > x^2$, so d is 1, hence $gcd(x, y) = 1$.
Next,

$$x^2 + ny^2 \equiv 0(modp) \tag{36.4}$$
$$x^2 \equiv -ny^2(modp) \tag{36.5}$$

Now it is clear that p couldnt devide y other wise $p|y \Rightarrow p|x$, and which is not possible.
Let $y'y \equiv 1(modp)$, then $(xy')^2 \equiv -n(modp)$, so $\left[\begin{array}{c} -n \\ p \end{array}\right] = 1$.

□

36.5 MultiplicativeFunction

Exercise 36.5 *Let $m,\ n \in N$ with $gcd(m,n) = 1$. Show that the positive divisors d of mn are precisely the numbers of the form kl where $k,\ l$ are any positive divisors of $m,\ n$ respectively, and that each d can be represented in this form in only one way.*
A function $f{:}N \to N$ is called a multiplicative function if $f(mn) = f(m)(n)$ whenever $gcd(m,n) = 1$. Let $\sigma(n)$ denote the sum af all positive divisors of n, and let $\tau(n)$ denote the number of positive divisors of n. Show that σ and τ are multiplicative functions.

Proof: As $gcd(m,n) = 1$, we can write $m = p_1^{e1} \dots p_r^{er}$ and $n = q_1^{f1} \dots q_s^{fs}$, where $p_1, \dots, p_r\ q_1, \dots, q_s$ are distinct primes and $e_1, \dots, e_r, f_1, \dots, f_s > 0$. By uniqueness fo prime factorisations, any positive divisor$d$ of mn can be written uniquely as $d = p_1 \dots p_r q_1 \dots q_s$ with $0 \leq a_i \leq e_i$ for each i and $0 \leq b_j \leq f_j$ for each j. Thus, writting $k = p_1^{a_1} \dots p_r^{a_r}$ and $l = q_1^{b_1} \dots b_s^{b_s}$, we have $d = kl$,with k, l positive divisors of m, n respectively.
Conversely if k, l are positive divisors of m, n respectively then clearly $d = kl$ is a positive divisors of mn. Each d has a unique representation in this form: by the unique factorisation of d into primes, each primes factors p_i, occurring in d must be a factor of k (since p_i does not divide n) and similarly each prime factor q_j in d must come from l.
Let by using the defination of $\sigma(n)$, that it demote the sum af all positive divisors of n, so.

$$\begin{aligned}
\sigma(mn) &= \sum_{d|mn} d && (36.6)\\
&= \sum_{k|l,l|n} kl && (36.7)\\
&= \left(\sum_{k|m} k\right)\left(\sum_{l|n} l\right) && (36.8)\\
&= \sigma(m)\sigma(n). && (36.9)
\end{aligned}$$

and,

$$\tau(mn) = \sum_{d|mn} 1 = \sum_{k|m}\sum_{l|n} 1 = \left(\sum_{k|m} 1\right)\left(\sum_{l|n} 1\right) = \tau(m)\tau(n) \qquad (36.10)$$

so both σ and τ are multiplicative function. □

Chapter 37

Sai Pramod Kumar

37.1 Congruences

Exercise 37.1 *(a)Suppose that m is either a power p^α of a prime $p > 2$ or else twice an odd prime power.Prove that, if $x^2 \equiv_m 1$, then either $x \equiv_m 1$ or $x \equiv_m -1$.*
(b)Prove that part (a) is always false if m is not of the form p^α or $2p^\alpha$.
(c)Prove that if m is an odd number which is divisible by r different primes, then the congruence $x^2 \equiv_m 1$ has 2^r different solutions for 0 and m.

Solution: (a)For example, suppose that $m = 2p^\alpha$.Since $m|(x^2 - 1) = (x + 1)(x - 1)$, we have α powers of p appearing in both $x + 1$ and $x - 1$ together. But since $p \geq 3$, it follows that p cannot divide both $x + 1$ and $x - 1$(which are only 2 apart from each other), and so all the $p's$ must divide one of them.
If $p^\alpha|x + 1$, then $x \equiv_{p^\alpha} -1$. If $p^\alpha|x - 1$, then $x \equiv_{p^\alpha} 1$. Finally, since $2|(x^2 - 1)$ it follows that x must be odd, i.e., $x \equiv_2 1 \equiv_2 -1$.
Using the property of congruences:If $a \equiv_m b$, $a \equiv_n b$ and m and n are relatively prime, then $a \equiv_{mn} b$, either $x \equiv_{2p^\alpha} 1$ or $x \equiv_{2p^\alpha} -1$.
(b)If x is not of the form p^α or $2p^\alpha$ or 4, the other possibilities are $m = 2^\alpha$ *where* $\alpha > 2$ or m=$p^\alpha m'$ *where* $m' \neq 2$
Case 1: Suppose $x = m/2 + 1$ where $m = 2^\alpha$
$x^2 = m^2/4 + 1 + m \equiv_m 1$
$\implies x \equiv_m 1$ *and* $x \equiv_m -1$
But $x = m/2 + 1 \implies x \not\equiv 1$ *or* $x \not\equiv -1$ which is a contradiction.

Therefore m can't be of the form 2^α.
Case 2: Suppose $m = p^\alpha m'$, *where* $m' > 2$ *and* $p^\alpha \parallel m$,
Using CRT, we can find a common solution for
$x \equiv_{p^\alpha} 1$ *and* $x \equiv_{m'} -1$
$\implies x^2 \equiv_{p^\alpha} 1$ *and* $x^2 \equiv_{m'} 1$
$\implies x^2 \equiv_{p^\alpha m'} 1 \equiv_m 1$
If $x \equiv_m 1 \implies x \equiv_{m'} 1$ *because* $gcd(m', p^\alpha) = 1$
Since x is a solution for $x \equiv_{m'} -1$, its a contraction for x to satisfy both $x \equiv_{m'} -1$ *and* $x \equiv_{m'} 1$

If $x \equiv_m -1 \implies x \equiv_{p^\alpha} -1$ again raising a contradiction

Therefore m can't be of the form $p^\alpha m'$.
Hence, part (a) is always false if m is not of the form p^α or $2p^\alpha$.

(c)$m = p_1 p_2 \dots p_r$ *where* $p_i's$ $1 \le i \le r$ are distinct primes
If $x^2 \equiv_m 1, \forall i.$
Let x_i' *and* x_i'' *be* 2 *solutions.* Let y_i be such that $y_i^2 \equiv_{p^i} 1$

$x \equiv_{p^1} y_1$
$\vdots$
$x \equiv_{p^r} y_r$
Using CRT, $x^2 \equiv_{p_i} y_i^2 \equiv_{p_i} 1 \Longrightarrow x^2 \equiv_m 1$

There are r equations and x an take 2 values for each equation. So, we have 2^r different sets of r equations giving 2^r different solutions.Each distinct value of x for an equation $x \equiv_{p_i} y_i$ yields a different solution because, if x_1 and x_2 yield the same solution then
$x_1 \equiv_m \; x_2 \Longrightarrow x_1 \equiv_{p_i} \; x_2 \equiv_{p_i} y_i \Longrightarrow x_1$ *and* x_2 are not different solutions.Therefore there are 2^r different solutions.

□

37.2 Infinite Continued Fractions

Exercise 37.2 *Prove that for* $n \ge 1$,

$$\xi - \tfrac{h_n}{k_n} = (-1)^n k_n^{-2} \; (\xi_{n+1} + <0, a_n, a_{n-1}, ..., a_2, a_1>)^{-1}$$

Solution:

$$\begin{aligned}
\xi - r_n &= \xi - \frac{h_n}{k_n} = \frac{\xi_{n+1} h_n + h_{n-1}}{\xi_{n+1} k_n + k_{n-1}} - \frac{h_n}{k_n} && (37.1)\\
&= \frac{k_n(\xi_{n+1} h_n + h_{n-1}) - h_n(\xi_{n+1} k_n + k_{n-1})}{k_n(\xi_{n+1} k_n + k_{n-1})} && (37.2)\\
&= \frac{-(h_n k_{n-1} - h_{n-1} k_n)}{k_n(\xi_{n+1} k_n + k_{n-1})} && (37.3)\\
&= \frac{-(-1)^{n-1}}{k_n(\xi_{n+1} k_n + k_{n-1})} (h_i k_{i-1} - h_{i-1} k_i = (-1)^{i-1}) && (37.4)
\end{aligned}$$

Claim 37.1 $k_n / k_{n-1} = <a_n, a_{n-1}, ..., a_2, a_1>$

Proof:

$$\begin{aligned} k_n/k_{n-1} &= \frac{a_n k_{n-1} + k_{n-2}}{k_{n-1}} && (37.5)\\ &= a_n + \frac{1}{k_{n-1}/k_{n-2}} && (37.6)\\ &= a_n + \frac{1}{a_{n-1} + \frac{1}{k_{n-2}/k_{n-3}}} && (37.7)\\ &= a_n + \cfrac{1}{a_{n-1} + \cfrac{1}{a_{n-2} + \cfrac{1}{\ddots + a_1 + \cfrac{k_{-1}}{k_0}}}} (k_{-1} = 0) && (37.8)\end{aligned}$$

$$=< a_n, a_{n-1}, ..., a_1 >$$

□

Continuing from Eqn. 37.8

$$= \frac{(-1)^n}{k_n(\xi_{n+1}k_n + k_{n-1})} \quad (37.9)$$

$$= \frac{(-1)^n}{k_n^2(\xi_{n+1} + k_{n-1}/k_n)} \quad (37.10)$$

$$= (-1)^n k_n^{-2}(\xi_{n+1} + < 0, a_n, a_{n-1}, ..., a_2, a_1 >)^{-1} \quad (37.11)$$

by using Claim 37.2, $k_{n-1}/k_n = \frac{1}{k_n/k_{n-1}} =< 0, a_n, a_{n-1}, .., a_2, a_1 >$

□

37.3 Diophantine Equations

Exercise 37.3 *Let a, b and c be positive integers such that $gcd(a, b) = 1$.Assuming that $c|ab$ is not an integer, prove that the number N of solutions of $ax+by = c$ in positive integers is $\lfloor c/ab \rfloor$ or $\lfloor c/ab \rfloor + 1$.Assumng furthur that c/a is an integer, prove that $N = \lfloor c/ab \rfloor$.*

Solution:

We know that $ax + by = c$ has solutions only if $gcd(a, b)|c$ and the solutions are of the form $x = x_1 + \frac{b}{g}t$ and $y = y_1 - \frac{a}{g}t$ where (x_1, y_1) is a solutions and $g = gcd(a, b)$.
For x to be positive, $t > -(g/b)x_1$
For y to be positive, $t > -(g/a)y_1$

We restrict t to the range $-(g/b)x_1 < t < (g/a)y_1$ for solutions to be in positive integers. The smallest allowable value for t is $\lfloor -(g/b)x_1 + 1 \rfloor$ and the largest value is $-\lfloor -(g/a)y_1 + 1 \rfloor$. The no.of solutions is then

$$\begin{aligned} N &= -\lfloor -(g/a)y_1 + 1 \rfloor - \lfloor -(g/b)x_1 + 1 \rfloor + 1 && (37.12)\\ &= -(\lfloor -(g/a)y_1 \rfloor + \lfloor -(g/b)x_1 + 1 \rfloor) && (37.13)\end{aligned}$$

Using theorem, $\lfloor x\rfloor + \lfloor y\rfloor \le \lfloor x+y\rfloor \le \lfloor x\rfloor + \lfloor y\rfloor + 1$, where x and y are real numbers. we get,

$$-(\lfloor -(g/a)y_1 - (g/b)x_1\rfloor + 1) \le N \le -(\lfloor -(g/a)y_1 - (g/b)x_1\rfloor)$$

Since $-(g/a)y_1 - (g/b)x_1 = -(g/(ab))(by_1 + ax_1) = -gc/(ab)$, we have

$$-\lfloor -gc/(ab)\rfloor - 1 \le N \le -\lfloor -gc/(ab)\rfloor$$

We have $g = 1$,
Case 1: if $c/(ab)$ is not an integer,
$-\lfloor -c/(ab)\rfloor - 1 \le N \le -\lfloor -c/(ab)\rfloor$
$-\lfloor -c/(ab)\rfloor - 1 = \lfloor c/ab\rfloor$
Therefore, the number of solutions N is $\lfloor c/ab\rfloor$ or $\lfloor c/ab\rfloor + 1$.

Case 2: if c/a is an integer,
Then a specific solution of $ax + by = c$ would be $x_1 = c/a$ and $y_1 = 0$.
$N = -(\lfloor -(g/a)y_1\rfloor + \lfloor -(g/b)x_1 + 1\rfloor) = -(\lfloor -c/(ab)\rfloor + 1) = \lfloor (c/(ab)\rfloor$
Therefore, the number of solutions N is $\lfloor c/(ab)\rfloor$.

□

37.4 Primitive Roots

Exercise 37.4 *Show that there are $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues for an odd prime p and find them.*

Solution:

Denote quadratic residues by r, nonresidues by n.
$r_1^{(p-1)/2} = 1$ *and* $r_2^{(p-1)/2} = 1$ implies that $r_1 r_2$ is also a quadratic residue.
$n_1^{(p-1)/2} = -1$ *and* $n_2^{(p-1)/2} = -1$ implies that $n_1 n_2$ is also a quadratic residue.
$r^{(p-1)/2} = 1$ *and* $n^{(p-1)/2} = -1$ implies that rn is a quadratic non residue.

Let g be the primitive root of an odd prime p.We have $g^{(p-1)/2} = -1$. We can infer that all the even powers of g,i.e $g^2, g^4, g^6..., g^{p-1}$, are quadratric residues because $(g^2)^{(p-1)/2} = g^{(p-1)/2}g^{(p-1)/2} = (-1)^2$. Similarly, $g^4, g^6, ..., g^{p-1}$ can be reduced to $(-1)^k$ where k is even. Hence they are quadratic residues.
Similarly, we can claim that $g^1, g^3, ..., g^{p-2}$ can be reduced to $(-1)^l$ where l is odd. Hence they are quadratic non-residues.

Using the theorem that if $gcd(a, n) = 1$ and let $a_1, a_2, ..., a_{\phi_n}$ be the positive integers less than n and relatively prime to n and a is a primiive root of n, then

$$a, a^2, ..., a^{\phi_n}$$

are congruent modulo n to $a_1, a_2, ..., a_{\phi_n}$ in some order.

Therefore, $g^1, g^2, g^3, ..., g^{(p-1)}$ are equivalent to 1,2,...(p-1) in some order and there are (p-1)/2 quadratic residues namely $g^2, g^4, g^6..., g^{p-1}$ and (p-1)/2 nonresidues namely $g, g^3, g^5, ..., g^{p-2}$.

□

37.5 Quadratic Reciprocity

Exercise 37.5 *Prove that* $\sum_{m=1}^{p} \left\lfloor \begin{array}{c} am+b \\ p \end{array} \right\rfloor = 0,$ *assuming* $a \not\equiv_p 0$*.Also prove that* $\left\lfloor \begin{array}{c} ab \\ p \end{array} \right\rfloor = \left\lfloor \begin{array}{c} a \\ p \end{array} \right\rfloor \left\lfloor \begin{array}{c} b \\ p \end{array} \right\rfloor$ *and* $\left\lfloor \begin{array}{c} a \\ p \end{array} \right\rfloor = \left\lfloor \begin{array}{c} b \\ p \end{array} \right\rfloor$ *if* $a \equiv_p b$ *.*

Solution: There is a one-to-one mapping between m and $am+b$. (For m_1, m_2, if $am_1 + b = am_2 + b \Longrightarrow m_1 \equiv_p m_2$ which is a contradiction).
Therefore

$$\sum_{m=1}^{p} \left\lfloor \begin{array}{c} am+b \\ p \end{array} \right\rfloor = \sum_{m=1}^{p} \left\lfloor \begin{array}{c} m \\ p \end{array} \right\rfloor$$

We know that there are $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues(shown in previous poblem). For all quadratic residues i, $\left\lfloor \begin{array}{c} i \\ p \end{array} \right\rfloor = 1$ and all quadratic nonresidues j, $\left\lfloor \begin{array}{c} j \\ p \end{array} \right\rfloor = -1$. Thus the sum is 0.

Furthur, $\left\lfloor \begin{array}{c} ab \\ p \end{array} \right\rfloor = (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} = \left\lfloor \begin{array}{c} a \\ p \end{array} \right\rfloor \left\lfloor \begin{array}{c} b \\ p \end{array} \right\rfloor$ and
$a \equiv_p b \Longrightarrow a^{(p-1)/2} \equiv_p b^{(p-1)/2} \Longrightarrow \left\lfloor \begin{array}{c} a \\ p \end{array} \right\rfloor = \left\lfloor \begin{array}{c} b \\ p \end{array} \right\rfloor$

□

Chapter 38

Tariq Aftab

38.1 Congruences of higher degree

Exercise 38.1 *Look at the following Definition and answer the following questions:*

Definition 38.1 *A series $\sum_{n=1}^{\infty} a_n \frac{z^n}{n}$ is H-entire if $a_n \in \mathbb{N}^+$ for all n. Two H-entire series series $\sum_{n=0}^{\infty} a_n \frac{z^n}{n}$ and $\sum_{n=0}^{\infty} b_n \frac{z^n}{n}$ are said to be congruent $(\underline{mod}\ \ n)$ if $a_n \equiv b_n (\underline{mod}\ n)$*

1. *Show that if $f(z)$ and $g(z)$ are H-entire series, then the same is true of*

$$f'(z),\ \int_0^z f(t)dt,\ f(z)g(z),\ \frac{f(z)^m}{m!}\ if\ f(0) = 0. \tag{38.1}$$

2. *Show that for any non-prime $m > 4$*

$$(e^z - 1)^{m-1} \equiv 0(\underline{mod}\ m) \tag{38.2}$$

In particular show that

$$(e^z - 1)^3 \equiv 2 \sum_{k=1}^{\infty} \frac{z^{2k+1}}{(2k+1)!} (\underline{mod}\ 4) \tag{38.3}$$

3. *For prime p, by using the periodicity $(\underline{mod}\ p)$ of the coefficients show that*

$$(e^z - 1)^{p-1} \equiv -\sum_{k=1}^{\infty} \frac{z^{k(p-1)}}{(k(p-1))!} \tag{38.4}$$

Solution:

1. Let $f(z) = \sum_{n=0}^{\infty} a_n \frac{z^n}{n!}$ and $g(z) = \sum_{n=0}^{\infty} b_n \frac{z^n}{n!}$. We then find that

$$f'(z) = \sum_{n=0}^{\infty} a_{n+1} \frac{z^n}{n!} \tag{38.5}$$

$$\int_0^z f(t)dt = \sum_{n=1}^{\infty} a_{n-1} \frac{z^n}{n!} \tag{38.6}$$

$$f(z)g(z) = \sum_{n=0}^{\infty}\sum_{m=0}^{n} a_m b_{n-m} \binom{n}{m} \frac{z^n}{n!} \tag{38.7}$$

Therefore all these series are H-entire.We now prove the final series to be H-entire using induction. Suppose $f(0) = 0$ and $\frac{f(z)^{m-1}}{(m-1)!}$ are H-entire.Since f and f' are H-entire the same is true for

$$\frac{f(z)^{m-1}}{(m-1)!} f'(z) \tag{38.8}$$

Therefore it is also true for

$$\int_0^z \frac{f(t)^{m-1}}{(m-1)!} f'(t)dt = \frac{f(z)^m}{m!} \tag{38.9}$$

Which proves the last equation to be H-entire by induction.

2. By part 1 we see that $(e^z - 1)^{m-1} = (m-1)!g(z)$ where $g(z)$ is H-entire, since for non-prime $m > 4$; $(m-1)! \equiv 0(\underline{mod}\ m)$\{let $m = pq$. Now if $p \neq q$ as both p and $q < (m-1)$ the result is obvious. If $p = q$ then we have the case that $m = p^2$ with p prime; if $p \neq 2$, p *and* $2p$ are both smaller than $(p^2 - 1)$ which is the result\}, we find

$$(e^z - 1)^m == \sum_{h=0}^{m} \binom{m}{h} e^{hz}(-1)^{m-h} = \sum_{n=0}^{\infty}[\sum_{h=0}^{m}(-1)^{m-h} \binom{m}{h} h^n]\frac{z^n}{n!} \tag{38.10}$$

\{We assume $0^0 = 1$\} therefore in particular we have

$$(e^z - 1)^3 = \sum_{n=1}^{\infty}[3 - 3 \times 2^n + 3^n]\frac{z^n}{n} \equiv [3 + 3^n]\frac{z^n}{n}(\underline{mod}\ 4) \tag{38.11}$$

Now we know that $3^2 \equiv 1(\underline{mod}\ 4)$, hence $3 + 3^{2p+1} \equiv 2(\underline{mod}\ 4)$ and $3 + 3^{2p} \equiv 0(\underline{mod}\ 4)$, which yields:

$$(e^z - 1)^3 \equiv 2\sum_{k=1}^{\infty} \frac{z^{2k+1}}{(2k+1)!}(\underline{mod}\ 4) \tag{38.12}$$

3. We now apply the formula with $m = p - 1$; and setting

$$(e^z - 1)^{p-1} = \sum_{n=1}^{\infty} a_n \frac{z^n}{n!}, \tag{38.13}$$

But the formula $h^{p-1} = 1(\underline{mod}\ p)$ implies that $a_{n+p-1} \equiv a_n(\underline{mod}\ p)$, and the coefficients are periodic; on the other hand, we know that $(p-1)! \equiv -1(\underline{mod}\ p)$, hence:

$$(e^z - 1)^{p-1} = z^{p-1} + \ldots \equiv (-1)\frac{z^{p-1}}{(p-1)!} + \ldots(\underline{mod\ p}) \tag{38.14}$$

Which definitely gives us

$$(e^z - 1)^{p-1} \equiv -\sum_{k=1}^{\infty} \frac{z^{k(p-1)}}{[k(p-1)]!}(\underline{mod}\ p) \tag{38.15}$$

□

38.2 Divisibility

Exercise 38.2 *Let $F_n = 2^{2^n} + 1$. Show that F_n divides $F_m - 2$ if $n < m$, and from this deduce that F_n and F_m are relatively prime if $m \neq n$. From the latter statement deduce a proof of the existence of an infinitude of primes.*

Solution: Let $k \in \mathbb{N}$ be such that $m = n + k$.Also let $u = 2^{2^n}$. We therefore have:

$$\frac{F_m - 2}{F_n} = \frac{F_{n+k} - 2}{F_n} = \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1} = \frac{u^{2^k} - 1}{u + 1} \tag{38.16}$$

But we know that

$$\frac{u^{2^k} - 1}{u + 1} = u^{2^k - 1} - u^{2^k - 2} + \ldots - 1 \tag{38.17}$$

Which is an integer.Hence F_n divides $F_m - 2$.Now let $d = gcd(F_n, F_m)$;since $d \mid F_n$ from above we have $d \mid F_m - 2$. Also since $d \mid F_m$ also we have $d \mid 2$. But because both F_n and F_m are odd, $d = 1$, and therefore F_n and F_m are relatively prime. We also see that the mapping of $\mathbb{N}$ into the set of prime numbers which assigns to each integer n the smallest prime factor of F_n is therefore injective, so there are indifinitely many prime numbers. □

38.3 Euler's Totient Function

Exercise 38.3 *We define*

$$N_k = e^{\sum_{p \leq x} logp} \tag{38.18}$$

With ϕ being the Euler's Function and $\nu(n)$ the number of prime factors of n, show that:

$$\nu(n) < k \; and \; \frac{\phi(n)}{n} > \frac{\phi(N_k)}{N_k} \; for \; n < N_k \tag{38.19}$$

Solution: Let $q = q_1^{a_1} q_2^{a_2} \ldots q_j^{a_j}$ be the prime factorization of n, with $q_1 \leq q_2 \leq \ldots \leq q_j$. Then we'll have

$$2 \leq q_1, 3 \leq q_2, \ldots, p_i \leq q_i \; for \; 1 \leq i \leq j \tag{38.20}$$

This implies that:

$$N_j = 2.3 \ldots p_j \leq n \tag{38.21}$$

Since by Hypothesis, $n < N_k$ and the sequence N_k is strictly increasing, we deduce that

$$j \leq k - 1 \; and \; since \; \nu(n) = j, \tag{38.22}$$

we have $\nu(n) < k$. Now

$$\frac{\phi(n)}{n} = \prod_{i=1}^{j} (1 - \frac{1}{q_i}) \tag{38.23}$$

$$\geq \prod_{i=1}^{j} (1 - \frac{1}{p_i}) \tag{38.24}$$

$$\geq \prod_{i=1}^{k-1} (1 - \frac{1}{p_i}) = \frac{\phi(N_{k-1})}{N_{k-1}} \tag{38.25}$$

And since we have

$$\frac{\phi(N_{k-1})}{N_{k-1}} = \frac{1}{(1 - \frac{1}{p_k})} \frac{\phi(N_k)}{N_k} > \frac{\phi(N_k)}{N_k} \tag{38.26}$$

Therefore we finally have

$$\frac{\phi(n)}{n} > \frac{\phi(N_k)}{N_k} \tag{38.27}$$

□

38.4 Fibonacci Numbers

Exercise 38.4 *Show that the Fibonacci Numbers* $(F_n)_{n\in\mathbb{N}}$*, where* $F_0 = 0$*,* $F_1 = 1$ *and for* $n \geq 0$*,* $F_{n+2} = F_{n+1} + F_n$*, is equidistributed* mod 5

Solution: We have mod 5: $F_0 = 0, F_1 = 1, \ldots, F_{20} = 0, F_{21} = 1$ and therefore for $n = 0$ and $n = 1$ we have $F_{n+20} = F_n$. By induction one deduces from this that the sequence is periodic with period 20. It only remains to be established by a further direct calculation that whenever $n \in \{0, 1, \ldots, 19\}$, F_n exactly every value mod 5 four times. More generally, F_n is periodic mod 5^k where ($k \geq 1$ is an integer.) with period 4.5^k and in each period it takes each value mod 5^k four times, hence it is equidistributed mod 5^k. In addition if F_n is equidistributed mod q where $q > 1$ *an integer*, q is necessarily of the form 5^k. □

38.5 Tchebychev's Theorem

Exercise 38.5 *The Prime Number Theorem states that*

$$\pi(x) = O(\frac{x}{logx}) \tag{38.28}$$

We define

$$\nu(x) = \sum_{p\leq x} logp \tag{38.29}$$

Show the equivalence of the Prime Number Theorem with

1. $\nu(x) \sim x$
2. $p_n \sim nlogn$ *(*p_n *being the* n^{th} *prime number)*

Solution:

1. We have

$$\nu(x) = \sum_{p\leq x} logp \leq logx \sum_{p\leq x} 1 = \pi(x)logx \tag{38.30}$$

Not $\forall\delta \in (0,1) : \nu(x) \geq \sum_{x^\delta<p\leq x} logp$

$$\geq \delta logx(\pi(x) - \pi(x^\delta)) \tag{38.31}$$

$$\delta\pi(x)logx - x^\delta logx \tag{38.32}$$

Assuming the *Prime Number Theorem* we deduce from this that

$$lim\lceil\frac{\nu(x)}{x}\rceil \leq 1 \; and \; lim\lfloor\frac{\nu(x)}{x}\rfloor \geq \delta \tag{38.33}$$

for all $\delta \in (0,1)$. Hence we have $lim\lfloor\frac{\nu(x)}{x}\rfloor \geq 1$ and therefore $\nu(x) \sim x$. Conversely if $\nu(x) \sim x$ we have using the first equation

$$lim\lfloor\frac{\pi(x)logx}{x}\rfloor \geq 1 \tag{38.34}$$

from which we have

$$x^\delta \sim \pi(x) \; and \; from \; lim\lceil\frac{\pi(x)logx}{x}\rceil \leq \frac{1}{\delta} \tag{38.35}$$

Which gives us the *Prime Number Theorem*

2. For each $n \geq 1$ we have $\pi(p_n) = n$. If the *Prime Number Theorem* is assumed, we have when $n \to \infty$

$$n \sim \frac{p_n}{logp_n} \tag{38.36}$$

$$logn \sim logp_n \; and \; p_n \sim nlogp_n \sim nlogn \tag{38.37}$$

Let's now assume that for all $x \geq 2$

$$P_{\pi(x)} \leq x \leq P_{\pi(x)+1} \tag{38.38}$$

If for infinite n we assume that $p_n \sim nlogn$ we deduce that for infinite x the extreme terms are equivalent to $\pi(x)log\pi(x)$ and consequently

$$x \sim \pi(x)log\pi(x) \tag{38.39}$$

And hence

$$logx \sim log\pi(x) \; and \; \pi(x) \sim \frac{x}{log\pi(x)} \sim \frac{x}{logx} \tag{38.40}$$

□

Chapter 39

Vikas Bansal

39.1 Generalisation of Euler's Thoerem *

Theorem 39.1 *Euler's generalisation of Fermat's theorem. If* $(a,k)=1$*, then*

$$a^{\phi(m)} \equiv 1(mod\ m).$$

Theorem 39.2 *Prove that* $a^{\lambda(n)} \equiv 1$ *(mod n), where*

$$n = p_1^{e_1} p_2^{e_2} \dots p_m^{e_m} \text{ is the prime expansion of } n,\ gcd(a,n)=1 \text{ and } \lambda(n) = lcm(\phi(p_1^{e_1}), \phi(p_2^{e_2}), \dots, \phi(p_m^{e_m})).$$

Proof: It is easy to see that $\phi(p_i^{e_i}) | \lambda(n)$ for each i. Also from Euler's generalisation of Fermat's Theorem defined above,

$$a^{\phi\left(p_i^{e_i}\right)} \equiv 1(\text{mod } (p_i^{e_i})) \text{ for each } i.$$

Raising to power $\frac{\lambda(n)}{\phi\left(p_i^{e_i}\right)}$, we get $a^{\lambda(n)} \equiv 1(\text{mod } (p_i^{e_i}))$ for each i.
$\Rightarrow (p_i^{e_i}) | \left(a^{\lambda(n)} - 1\right)$ for each i. Since $p_i^{e_i}$'s are coprime, their product also divides $\left(a^{\lambda(n)} - 1\right)$.
Hence

$$\begin{aligned} n &\quad | \left(a^{\lambda(n)} - 1\right) \\ \Rightarrow &\quad a^{\lambda(n)} \equiv 1(\text{mod } n). \end{aligned}$$

□

39.2 Primes and Congruence

Example 39.1 *Let* p *and* q *be primes. If* p^2 *divides* $2^q - 1$*, then* $2^{\left(\frac{p-1}{2}\right)} \equiv 1(\ mod\ p^2)$ *and moreover* $2^{p-1} \equiv 1$ *(mod* p^2*).*

Proof: If p divides $2^q - 1$, then $2^q \equiv 1$ (mod p). Let d be the algebraic order of the group 2(modulo p). Then d divides the prime q hence it must be q itself.
Using Fermat's little theorem, $2^{p-1} \equiv 1$ (mod p) and d also divides $(p-1)$. Since $(p-1)$ is even we get, $q|(p-1)$.

Or, $p = 2kq + 1$ for some integer k. Hence $2^q = 2^{\left(\frac{p-1}{2k}\right)} \equiv 1 \pmod{p^2}$.
Raising to k^{th} power we get,

$$2^{\frac{p-1}{2}} \equiv 1 (\bmod p^2).$$

Squaring this equation (modulo p^2) completes the proof.

Example 39.2 *Prove that n divides $N = \sum_{r=1} n - 3r(r!)$ iff n is a prime number.*

Proof: $N = 1(1!) + 2(2!) + \ldots + (n-3)[(n-3)!]$. $r(r!)$ can be written as $(r+1)! - r!$.Therefore

$$N = (2! - 1!) + (3! - 2!) + \ldots + [(n-2)! - (n-3)!] = (n-2)! - 1.$$

Multiplying through by $n - 1$ and adding n to both sides, we get

$$(n-1)N + n = (n-1)! + 1.$$

Using Wilson's Theorem that n is a prime iff n divides $(n-1)! + 1$, from the above equation we get n is prime iff n divides $(n-1)N$. But n and $n-1$ are always relatively prime, so n divides N. □

□

39.3 Diophantine Equations

Example 39.3 *If y and z are natural numbers satisfying*

$$y^3 + 4y = z^2.$$

prove that y is of the form $2k^2$.

Proof: Let k^2 denote the greatest square which divides k and let $y = nk^2$. Then n cannot have repeated factors, o/w a square greater than k^2 would divide y.

$$y^3 + 4y = z^2.$$

gives

$$y(y^2 + 4) = z^2,$$
$$nk^2(y^2 + 4) = z^2,$$

hence

$$k^2 | z^2 \Rightarrow k | z.$$

Let $z = mk$. Then $nk^2(y^2 + 4) = z^2 \Rightarrow n(y^2 + 4) = m^2$. Or $n(y^2 + 4)$ is a perfect square. But according to assumption, n does not have repeated factors. Thus all the factors of n must occur again in $y^2 + 4$.i.e.

$$n | (y^2 + 4).$$

Also since $y = nk^2$, $n | n^2k^4 + 4$, and $n | 4$. Hence $n = 1, 2$ or 4. Since n has no repeated factors, $n \neq 4$. If $n = 1$, then $y^2 + 4 = m^2$. But no two squares differ by 4. Hence n has to be 2 for any solutions to exist. Hence y is of the form $2k^2$.

□

39.4 Chinese Remainder Theorem

Example 39.4 *A square free integer is an integer n which is not divisible by the square of a prime. Show that* $\forall\ k$, $\exists\ m$ *such that* $m+1,\ m+2,\ \dots\ m+k$ *are all not square free.*

Proof: Choose $p_1, p_2, \dots p_k$ to be k distinct primes,for any given k. Consider the k congruences,

$$x \equiv -1 (\text{mod } p_1^2).$$
$$x \equiv -2 (\text{mod } p_2^2).$$
$$x \equiv -3 (\text{mod } p_3^2).$$
$$\vdots$$
$$x \equiv -k (\text{mod } p_k^2).$$

Using the Chinese Remainder Theorem, these congruences have common solutions. Consider any solution x. We obtain, $p_1^2|(x+1)$, $p_2^2|(x+2)$, $\dots p_k^2|(x+k)$. Hence each of $x+1$, $x+2$, $\dots$ $x+k$ is divisible by a square of a prime. Therefore x is the required solution.

□

39.5 Algebraic Number Theory (Fields)

Example 39.5 *Prove that for any prime* $p > 2$ *the sum*

$$\frac{1}{1^3} + \frac{1}{2^3} + \frac{1}{3^3} + \dots + \frac{1}{(p-1)^3}$$

if written as a rational number a/b *has the property that* $p|a$.

Theorem 39.3 $\mathbb{Z}_p$ *is a field iff m is a prime number.*

Proof: Consider the field $\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is a field, each element (except 0) of $\mathbb{Z}_p$ has a multiplicative inverse. Therefore the term $1/a^2$ in the field $\mathbb{Z}_p$ can be written as b^2 where b is the multiplicative inverse of a in $\mathbb{Z}_p$.Hence in the field $\mathbb{Z}_p$ the equivalent problem is *"Prove that the sum* $\frac{1}{1^3} + \frac{1}{2^3} + \frac{1}{3^3} + \dots + \frac{1}{(p-1)^3}$ *is the zero element of the field"*. But the inverses of the elements 1,2,3 $\dots, p-1$ are the same elements in some order. So the sum $\frac{1}{1^3} + \frac{1}{2^3} + \frac{1}{3^3} + \dots + \frac{1}{(p-1)^3}$ can be written as $1^3 + 2^3 + 3^3 + \dots + (p-1)^3 = \frac{p^2(p-1)^2}{4} = a$. Since p is a prime, $(p-1)^2$ is divisible by 4. Therefore this sum is zero in $\mathbb{Z}_p$, except in the case $p = 2$ when divisibility by 4 will not hold.

□

39.6 Greatest Integer Function

Example 39.6 *Let* $\mathbb{S}$ *be the set of integers given by* $[n\alpha]$ *and* $[n\beta]$ *for* n = *1,2,3* $\dots$, *where* [] *denotes the Greatest Integer Function. Prove that* $\mathbb{S}$ *consists of every positive integer, each appearing exactly once, if* α *and* β *are positive irrational numbers such that* $\frac{1}{\alpha} + \frac{1}{\beta} = 1$.

Proof: Suppose there is an integer k which does not belong to $\mathbb{S}$. Hence $\exists$ an integer n such that

$$n\alpha < k \text{ and } (n+1)\alpha > k+1. \tag{39.1}$$

Similarly $\exists$ an integer m such that

$$m\beta < k \text{ and } (n+1)\beta > k+1. \tag{39.2}$$

Using the properties of the Greatest Integer Function. Using the above inequalities 1.10 and 1.11, we get

$$\begin{aligned} n+m &< \frac{k}{\alpha}+\frac{k}{\beta} && (39.3)\\ \text{and } (n+1)+(m+1) &> \frac{k+1}{\alpha}+\frac{k+1}{\beta}. && (39.4)\\ \Rightarrow (n+m) &< k \text{ and } (n+m+1) > k. && (39.5)\\ \Rightarrow (k-1) &< (n+m) < k. && (39.6) \end{aligned}$$

Which is a contradiction since $(m+n)$ is an integer and it cannot lie between two consecutive integers. Now we prove that $\exists$ no integer which appears more than once.Suppose on the contrary this holds, i.e

$$\begin{aligned} \exists \quad & k \text{ such that } [n\alpha] = [m\beta] = k. && (39.7)\\ \Rightarrow \quad & \frac{k}{\alpha} < n < \frac{k+1}{\alpha} \text{ and } \frac{k}{\beta} < m < \frac{k+1}{\beta}. && (39.8)\\ \Rightarrow \quad & k < n+m < k+1. \text{ (adding the equations from 1.17)} && (39.9) \end{aligned}$$

Which is a contradiction (same as above). Hence the result holds. □

Chapter 40

Anuj Saxena

40.1 Chinese Remainder Theorem

Exercise 40.1 *(Genralization of CRT)*

Let $m_1, m_2, \ldots, m_k$ be positive integers.Then Given integers $x_1, x_2, \ldots, x_k$,the system of congruences

$$x \equiv x_i (mod\ m_i) \quad 1 \leq i \leq k$$

has a solution iff $x_i \equiv x_j \quad (mod\ gcd(m_i, m_j))$ forall $i \neq j$.Moreover if solution exist it is unique (mod lcm($m_1, m_2, \ldots, m_k$)).

Proof:

Suppose the solution of the system exist we have to show that $x_i \equiv x_j \pmod{\gcd(m_i, m_j)}$. we have,

$$\begin{aligned} x &\equiv x_i (mod\ m_i) \\ and \quad x &\equiv x_j (mod\ m_j) \end{aligned}$$

where $1 \leq i, j \leq k$ and $i \neq j$. clearly,

$$\begin{aligned} x &\equiv x_i (mod\ gcd(m_i, m_j)) \\ and \quad x &\equiv x_j (mod\ gcd(m_i, m_j)) \end{aligned}$$

Since solution of the system exist

$$\Rightarrow x_i \equiv x_j (mod\ gcd(m_i, m_j))$$

Conversely, given $x_i \equiv x_j \pmod{\gcd(m_i, m_j)}$ we have to show that the solution of the system exist.

we will prove this by constructing the solution of the system using given condition.For this we will first take a pair of congruence and reduce it into a single congruence.

Suppose we have a pair

$$x \equiv x_1 (mod\ m_1) \qquad x \equiv x_2 (mod\ m_2)$$

Then $x = x_1 + km_1$ for some k.Since $x \equiv x_2 \pmod{m_2}$, This implies

$$\begin{aligned} x_1 + km_1 &= x_2 \qquad (mod\ m_2) \\ or \quad km_1 &= x_2 - x_2 \quad (mod\ m_2) \end{aligned}$$

let $d = gcd(m_1, m_2)$ then $d \mid x_2 - x_1$.Thus,

$$k\frac{m_1}{d} = \frac{x_2 - x - 1}{d} \ (mod\ m_2/d)$$

Since we know if $gcd(a, n) = d$ then the congruence $ax \equiv b$ (mod n) has a solution iff $d \mid b$ and solution is unique modulo n/d, this implies that the congruence has a unique solution $t \equiv t_1$ (mod m_2/d).Substituting $k = k_1 + jm_2/d$ in $x = x_1 + km_1$ we find $x = x_1 + k_1m_1 + jm_1m_2/d$.Hence $x = x_1 + k_1m_1$ (mod lcm(m_1, m_2)).

By repeating the process $k - 1$ times, we find the solution to a system of k congruences.

To prove uniqueness, Suppose system has two solutions x and y s.t.

$$\begin{aligned} x &= x_i(mod\ m_i) \quad 1 \le i \le k \\ and \quad y &= x_i(mod\ m_i) \quad 1 \le i \le k \end{aligned}$$

then $x - y \equiv 0$ (mod m_i) for $1 \le i \le k$, hence $x \equiv y$ (mod lcm$(m_1, m_2, \ldots, m_k)$). □

40.2 Euler's ϕ-Function

Definition 40.1 *(Generalization of Euler's ϕ-function)*

Let $a_1, a_2, \ldots, a_k$ be a set of arbitrary integers.Define

$$\psi(n; a_1, a_2, \ldots, a_k) = \mid \{h \mid 1 \le h \le n, h + a_i \text{is relative prime to } n \text{ for all } i,\ 1 \le i \le k\} \mid$$

also denoted simply by $\psi(n)$

Example 40.1 *For example if $a_1 = 0$,$a_2 = 1$ for $k = 2$ and $n = 15$, then $\psi(15)$ is the number of h , $1 \le h \le 15$, for which h+0 , h+1 both relative prime to 15. Since there are only three such values of h (namely $h = 1, 7, 13$), $\Rightarrow \psi(15; 0, 1) = \psi(15) = 3$.*

Fact 40.1 *for $a_1, a_2, \ldots, a_k = 0$, $\psi(n) = \phi(n)$.*

Exercise 40.2 *(i) For relative prime numbers , ψ is multiplicative function. i.e.If (m,n)=1, $\psi(mn) = \psi(m)\psi(n)$.*

(ii) If canonical form of the n is $p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}$ and if $t_i, 1 \le i \le r$,denotes the number of integers among $e_1, e_2, \ldots, e_k$ which are incongruent modulo p_i, then

$$\begin{aligned} \psi(n) &= \frac{n}{p_1p_2\ldots p_r}(p_1 - t_1)(p_2 - t_2)\ldots(p_r - t_r) \\ &= n(1 - \frac{t_1}{p_1})(1 - \frac{t_2}{p_2})\ldots(1 - \frac{t_r}{p_r}) \end{aligned}$$

Proof:

(i) Choose integers r and s such that,

$$\begin{aligned} r \equiv 1(mod\ m), &\qquad r \equiv 0(mod\ n) \\ s \equiv 0(mod\ m), &\qquad s \equiv 1(mod\ n) \end{aligned}$$

Then as x and y ranges over the complete set of residues $1, 2, \ldots, m$ modulo m and $1, 2, \ldots, n$,modulo n respectively , the mn numbers

$$z = rx + sy(mod\ mn)$$

ranges over a complete set of residue , modulo mn.

For if ,

$$\begin{aligned} rx_1 + sy_1 &\equiv rx_2 + sy_2 (mod\ mn) \\ \Rightarrow r(x_1 - x_2) &\equiv s(y_2 - sy_1)(mod\ mn) \end{aligned}$$

i.e.

$$\begin{aligned} r(x_1 - x_2) &\equiv s(y_2 - sy_1)(mod\ m) \\ and\ r(x_1 - x_2) &\equiv s(y_2 - y_1)(mod\ n) \end{aligned}$$

Consequently , $x_1 \equiv x_2 (mod\ m)$ and $y_2 \equiv y_1 (mod\ n)$ and the mn values of the z form a complete set of residue ,modulo mn.

Hence for each a_i , $1 \leq i \leq k$, there exist a pair of integers x_i and y_i, Such that

$$a_i \equiv rx_i + sy_i (mod\ mn)$$

i.e.

$$\begin{aligned} a_i &\equiv 1.x_i (mod\ m) \\ and\ a_i &\equiv 1.y_i (mod\ n) \end{aligned}$$

Now , we get

$$z + a_i \equiv r(x + x_i) + s(y + y_i)(mod\ mn)$$

We know that $z + a_i$ is relative prime to mn iff it is relative prime to both m and n

Now, $z + a_i$ is relative prime to m iff $x + x_i$ is relative prime to m , and $z + a_i$ is relative prime to n iff $y + y_i$ is relative prime to n.

This showes that $x + a_i$ is relative prime to m and $y + a_i$ is relative prime to n.This occurs for all $i = 1, 2 \ldots, k$ simultaneously for all $\psi(m)$ values of x of the set $1, 2, \ldots, m$ and for all $\psi(n)$ values of y of the set $1, 2 \ldots, n$.

This gives $\psi(m)\psi(n)$ as the number of permissible values of z for which the $z + a_1, z + a_2, \ldots, z + a_k$ are relative prime to mn, which is $\psi(mn)$.Hence proved.

(ii) First we will show that for power of prime, i.e for $n = p^\alpha$ and $\alpha \geq 1$, value of $\psi(p^\alpha) = p^{\alpha-1}(p - t)$, where t is number of distinct residues modulo p among $a_1, a_2 \ldots, a_k$.

Let $r_1, r_2, \ldots, r_t$ be the non-negative residue , modulo p of $a_1, a_2 \ldots, a_k$.And arrange the number n in p^α rows each having n integers as

$$\begin{matrix} 1 & 2 & \cdots & p-1 & p \\ p+1 & p+2 & \cdots & 2p-1 & 2p \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ (p^{\alpha-1}p+1) & (p^{\alpha-1}p+2) & \ddots & (p^\alpha - 1) & p^\alpha \end{matrix}$$

Then in the first row there are $p - t$ integers incongruent modulo p to the $-r_1, -r_2, \ldots, -r_t$ s.t. $h + r_1, h + r_2, \ldots, h + r_t$ are relative prime to p (and so relative prime to p^α).

Also each number in a column headed by one of these $p - t$ integers h would provide an h s.t. $h + r_i, 1 \leq i \leq t$, are each relative prime to p.Thus $\psi(p^\alpha) = p^{\alpha-1}(p - t)$.

Now ,Since ψ is multiplicative function,

$$\begin{aligned}
\psi(n) &= \psi(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}) \\
&= \psi(p_1^{\alpha_1})\psi(p_2^{\alpha_2})\dots\psi(p_r^{\alpha_r}) \\
&= p_1^{\alpha_1-1}(p_1-t_1)p_2^{\alpha_2-1}(p_2-t_2)\dots p_r^{\alpha_r-1}(p_r-t_r) \\
&= \frac{n}{p_1p_2\dots p_r}(p_1-t_1)(p_2-t_2)\dots(p_r-t_r) \\
&= n(1-\frac{t_1}{p_1})(1-\frac{t_2}{p_2})\dots(1-\frac{t_r}{p_r})
\end{aligned}$$

□

40.3 General Number Theory

Definition 40.2 *(Farey Sequences)*

Farey sequence of order n is the increasing sequence of the irreducible rational fractions between 0 and 1, both inclusive, whose denominators do not exceeds n..

Example 40.2 *For example , Farey sequence of order 6 is*

$$\frac{0}{1},\frac{1}{6},\frac{1}{5},\frac{1}{4},\frac{1}{3},\frac{2}{5},\frac{1}{2},\frac{3}{5},\frac{2}{3},\frac{3}{4},\frac{4}{5},\frac{5}{6},\frac{1}{1}$$

Exercise 40.3 *(i) if a_1/b_1 and a_2/b_2 be two consecutive terms in farey sequence,then $a_2b_1 - a_1b_2 = 1$.*

(ii) if $a_1/b_1, a_2/b_2$ and a_3/b_3 are three consecutive terms of Farey sequence,then $a_2/b_2 = (a_1 + a_3)/(b_1 + b_3)$.

(iii) Two consecutive term of a Farey sequence of order n , for n greater then 1,have different denominators.

(iv) Prove that the number of terms in the Farey sequence of order n is $1+\phi(1)+\phi(2)+\ldots+\phi(n)$, where $\phi(k)$ denotes Euler's ϕ-function.

Proof:

(*i*) Since first two terms of any Farey sequence are $0/1$ and $1/n$ so the result holds when n=1.Next, let $n > 1$.Let a_1/b_1 and a_2/b_2 are terms in Farey sequence.Since the fractions in the sequence are in their lowest terms i.e. $(a_1, b_1) = (a_2, b_2) = 1$.This showes that there exist a solution $x = x_0$ and $y = y_0$ of the equation

$$b_1x + (-a_1)y = 1$$

and so the general solution ,for t arbitrary integer , are $x = x_0 + a_1t$ and $y = y_0 + b_1t$

Sice the set on integer $w, n - b_1 < w \le n$, form a complete set of residues, modulo b_1 , choose t so that $n - b_1 < y_0 + b_1t \le n$.Now since a_1, b_1 and y are all positive integers,we have from equation $bx = 1 + ay$ that $x > 0$. Moreover since $b_1x = 1 + a_1y \le 1 + a_1n$,we have

$$x \le \frac{1 + a_1n}{b_1} \le \frac{1 + (b_1 - 1)n}{b_1} < n$$

Hence,since $(x, y) = 1, 0 \le n - b_1 < y \le n$ and $0 < x < n$ this implies x/y is a term in the farey sequence of order n.Now from $b_1x + (-a_1)y = 1$, we have

$$\frac{x}{y} - \frac{a_1}{b_1} = \frac{1}{b_1y} > 0$$

and so

$$x - y = \frac{1 + a_1 y - b_1 y}{b_1} \leq \frac{1 - y}{b_1} \leq 0$$

if x/y is not the successor of a_1/b_1,

$$\frac{x}{y} - \frac{a_2}{b_2} = \frac{b_2 x - a_2 y}{b_2 y} \geq \frac{1}{b_2 y}$$

On the other hand,

$$\frac{a_2}{b_2} - \frac{a_1}{b_1} \geq \frac{1}{b_1 b_2} \Rightarrow \frac{x}{y} - \frac{a_1}{b_1} \geq \frac{b_1 + y}{b_1 b_2 y} > \frac{n}{b_1 b_2 y}$$

however,

$$\frac{1}{b_1 y} = \frac{x}{y} + \frac{a_1}{b - 1} > \frac{n}{b_1 b_2 y} ge \frac{1}{b_1 y}$$

Which is a contradiction.Therefore x/y must be a_2/b_2 and so $a_2 b_1 - a_1 b_2 = 1$.

(ii) The result follows from the last result , by applying it for two terms at a time and by simple manipulation.

(iii) Let a_1/b_1 and a_2/b_2 be two consecutive terms of the sequence.Given $n > 1$, so there are atleast three terms in the Farey sequence of order n.If a_1/b_1 is the first term, the next term will be $1/n$.If a_2/b_2 is the last term of the sequence , a_1/b_1 is $(n-1)/n$ and a_2/b_2 is $1/1$

Assume that $b_1 > 1$. If $b_1 = b_2$, then $b_1 > a_2 \geq a_1 + 1$ and since $a_1 < a_2 \leq b_1 - 1$

$$\frac{a_1}{b_1} < \frac{a_1}{b_1 - 1} < \frac{a_1 + 1}{b_1} \leq \frac{a_2}{b_2}$$

Since $0 < a_1/(b_1 - 1) < 1$,we have a term of the sequencse between two consecutive terms of the sequence. This is a contradiction to our assumption that $b_1 = b_2$

(iv) Proof followe from the facts that if a/b is an element in Farey sequence then $(a, b) = 1$, and for any b(denominator) , $1 \leq b \leq n$ the possible a s.t a/b is an element in Farey sequence are $\phi(a)$ exactly. □

40.4 Quadratic Residue

Exercise 40.4 *(Sum of Two Squares)*

Let the positive integer $n = lm^2$, where l is not divisible by the square of a prime .Then n can be written as a sum of two squares iff l contains no prime factor of the form $4m + 3$.

Answer For example $20 = 5.2^2 = 4^2 + 2^2$ and $90 = 2.3^2.5 = 9^2 + 3^2$ but $12 = 3.2^2$ can not be written as a sum of two squares.

Claim 40.1 *If $m > 1$ and if k is the least integer greater than $\sqrt{m}$, then for an integer a relative prime to m there exist positive integers x and y , $0 \leq x, y \leq k - 1$, such that either $ay \equiv x (mod\ m)$ or $ay \equiv -x\ (mod\ m)$*

Proof: Consider the set $S = \{ay + x | 0 \leq x, y \leq k - 1\}$. Note that m lies between squares of $k - 1$ and k i.e $(k-1)^2 \leq m < k^2$. Observe that $k = 2$ for $m = 2$, $k = 2$ for m = 3 , and $k \leq (k-1)^2$ when $k \geq 3$.This showes that $k \leq m$ for $m \geq 2$.

Since the cardinality of S is k^2 $(> m)$, atleast two of them must belong to same residue class modulo m.Suppose

$$ay_1 + x_1 \equiv ay_2 + x_2 (mod\ m)$$

we then have

$$a(y_1 - y_2) \equiv x_2 - x_1 (mod\ m)$$

Since $y1 \not\equiv y_2(mod\ m)$ and $x_1 \not\equiv x_2(mod\ m)$ (by assumption) , set $x =\mid x_2 - x_1 \mid$ and $y =\mid y_1 - y_2 \mid$ where $1 \leq x, y \leq k-1$.Then we have solutions x and y of either $ay \equiv x$ (mod m) when $y_1 - y_2$ and $x_2 - x_1$ have sign or $ay \equiv -x$ (mod m) when $y_1 - y_2$ and $x_2 - x_1$ have opposite signs. □

Claim 40.2 *The product of two sum of two squares is sum of two squares.*

Proof: Proof is direct from the identity

$$(p^2 + q^2)(r^2 + s^2) = (pr + qs)^2 + (ps - qr)^2$$

□

Corollary 40.1 *If each $m_1, m_2 \ldots, m_k$,$\forall k \geq 2$, is a sum of two squares ,then $m_1.m_2 \ldots m_k$ is also a sum of two squares.*

Claim 40.3 *Every prime m of the form $4k + 1$ can be written as a sum of two squares.*

Proof: Since -1 is a quadratic residue of $m = 4k + 1(?)$,

$$a^2 + 1 \equiv 0 (modm)$$

is solvable.By claim 0.1 there exist positive integer x and y , each less than $\sqrt{m}$, s.t.

$$ay \equiv \pm x(modm)$$

Now ,

$$a^2y^2 + y^2 \equiv 0(modm) \Rightarrow x^2 + y^2 \equiv 0(modm)$$

Hence

$$x^2 + y^2 = mn$$

where $n \geq 1$. But , since $x^2 + y^2 < 2m$, $p = x^2 + y^2$. □

Now we will prove the main result by usying these three claims-

Since

$$w^2 \equiv \begin{cases} 0(mod4) & \text{when w is even} \\ 1(mod4) & \text{when w is odd} \end{cases}$$

This implies for any x and y , $x^2 + y^2 \not\equiv 3$ (mod 4). Hence , no prime of the form $4m + 3$ can be written as a sum of two squares.Moreover every prime not of the form 4m +3 can be written as the sum of the two squares, since $2 = 1^2 + 1^2$.

$\Rightarrow$

Suppose that $n = lm^2$ is a sum of two squares , we have to show that l can not have a prime factor of the form $4m + 3$.

This is obvious for $l = 1$ and $l = 2$. Take $l \geq 3$. Let $n = lm^2 = a^2 + b^2$, where $ab \neq 0, d = (a, b), a = da_0, b = db_0, (a_0, b_0) = 1$

If $d > 1$, let $d = q^r d_1$ where $r \geq 1$ and $(d_1, q) = 1$.Since $d^2 \mid n$, $q \mid m$ and $m = q^s m_1$, where $(m_1, q) = 1$.If $r > s$, then $2r \geq 2s + 2$. Since the highest power of q deviding lm^2 is not greater than $2s + 1$, $2r \leq 2s + 1$.This is a contradiction. Hence , since $d^2 \mid n$ and $r \leq s$, we see that $d^2 \mid m^2$.say $m^2 = d^2 m_0^2$.This showes , since

$$lm_0^2 = \frac{a^2 + b^2}{d^2} = a_0^2 + b_0^2$$

we have $a_0^2 + b_0^2 \equiv 0(modl)$. Next, let p be an odd prime factor of l. Since $(a_0, b_0) = 1$,$(a_0 b_0, p) = 1$.Let c satisfy the congruence $a_0 c \equiv 1(modp)$.Then, since $a_0^2 + b_0^2 \equiv 0(modp)$,

$$(a_0 c)^2 + (b_0 c)^2 \equiv 0(modp) \Rightarrow (b_0 c)^2 \equiv -1(modp)$$

Now since -1 is quadratic residue of p, p must be of the form $4m + 1$.

$\Leftarrow$

now we will show that ,when l contains no square of a prime and no prime factor of the form $4m + 3$, $n = lm^2$

$case1$: when $l = 1$, we have $n = m^2 + 0^2$

$case2$: when $l > 1$, let $l = p_1 p_2 \ldots p_k$ be canonical decomposition of l.Each of these prime is either 2 or of the form $4m + 1$ and so a sum of two squares. Hence from $claim0.2$, l is a sum of two squares , say $l = p^2 + q^2$.Therefore

$$n = lm^2 = (pm)^2 + (qm)^2$$

Fact 40.2 *The Diophantine equation $n = x^2 + y^2$ is solvable in integers iff n has the property stated above.*

40.5 Sylow Theorem

Theorem 40.3 *If p is a prime and $p^\alpha \mid\mid \mathcal{O}(G)$ then G has a subgroup of order p^α , called Sylow p-subgroup G or just Sylow subgroup.*

Exercise 40.5 *Using Sylow Theorem prove that,*

(i) If a prime p divides the order of a finite group G $(= p^\alpha m, (p, m) = 1)$, then G contain an element of the order p.

(ii) using part (i), prove that there are exactly two isomorphism classes of groups of order 6.

Proof: (i) From Sylows theorem, let H be a subgroup of order p^α and let x be an elemet of H s.t. $x \neq 1(identity)$. Since we know that the order of a element divides the order of the groups , this implies that x divides p^α so it is p^r for some r , $0 < r \leq \alpha$.Then $x^{p^{r-1}}$ has order p.

(ii)According to claim(i) a group of order 6 must contain an element of order 3 and an element of order 2.Let x be an element of order 3 and y be an element of order 2 in G s.t.

$$G = \{x^i y^j \mid 0 \leq i \leq 2, 0 \leq j \leq 1\}$$

form a distinct element of group.For if $x^i y^j = x^p y^q$ this implies $x^{i-p} = y^{q-j}$.Every power of x except the identity has order 3, and every power of y except the identity has order 2.Thus $x^{i-p} = y^{q-j} = 1$, which shows that $p = i$ and $q = j$.Since G has order 6, the six element $1, x, x^2, y, xy, x^2y$ run through the whole group.In particular, yx must be one of them.

clearly $yx \neq y$ because this will imply that $x = 1$, also $y \neq 1, x, x^2$ for similer reasons.Therefore,

$$either \quad yx = xy \quad or \quad yx = x^2y$$

holds in G.Either of these relations , together with $x^3 = 1$ and $y^2 = 1$ form the multiplication table for the group.Therefore there are atmost two isomorphism classes of order 6. □